(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年7 月15 日 (15.07.2004)

PCT

(10) 国際公開番号
WO 2004/059925 A1

(51) 国際特許分類[7]: H04L 12/56

(21) 国際出願番号: PCT/JP2003/016538

(22) 国際出願日: 2003 年12 月24 日 (24.12.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-371448
2002 年12 月24 日 (24.12.2002) JP

(71) 出願人 および
(72) 発明者: 福嶋 一 (FUKUSHIMA,Hajime) [JP/JP]; 〒165-0027 東京都 中野区 野方二丁目６２番３号 Tokyo (JP).

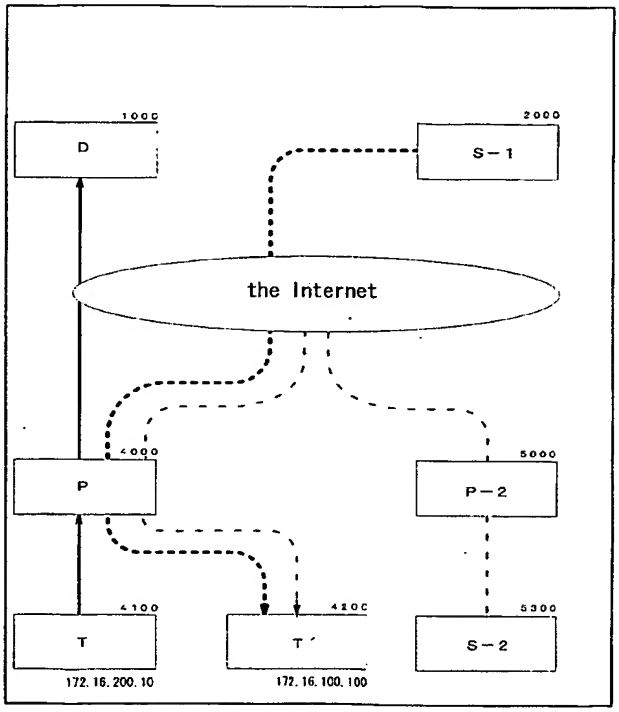
(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

/続葉有/

(54) Title: COMMUNICATION MODEL, SIGNAL, METHOD, AND DEVICE FOR CONFIRMING REACHABILITY IN NETWORK WHERE HOST REACHABILITY IS ACCOMPLISHED BY RELATING STATIC IDENTIFIER TO DYNAMIC ADDRESS

(54) 発明の名称: 静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる網にあって、到達性を確認するための通信モデル、信号、方法および装置



(57) Abstract: In a network where host reachability is accomplished by relating a static identifier to a dynamic address, the live/death of a communication node and reachability are confirmed by using a sign and countersign.

(57) 要約: 静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる網にあって、サイン・アンド・カウンターサインを用いて、通信ノードの活死および到達性を確認する。

WO 2004/059925 A1

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明細書

発明の名称)

静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる網にあって、到達性を確認するための通信モデル、信号、方法および装置

技術分野)

本発明は、蓄積交換型の通信網において、あて先端末を発見する過程における不備を解決する通信モデル、信号、方法および装置に関する。

詳しくは、静的な識別子を動的な住所に変形することによって、あて先端末への到達性を発信元に提供する場合において、発信元があて先端末への誤った到達性を持つ場合と正しい到達性を持つ場合とを峻別する。

背景技術)

特許文献1) 特許公表 2001-519607 亦はWO 99／18515 米インテル)静的な識別子を動的に割当てられたネットワーク・アドレスに変形する方法および装置

特許文献2) 特開 2001-135301 (NTT) IPアドレス情報通知方法およびIPアドレス情報通知装置並びにこのプログラムを記憶した記憶媒体

特許文献3) 特開 2002-318737 (インデックス)管理サーバ

特許文献4) 特開 2002-281032 東芝)監視対象切替プログラム、方法及び監視システム

特許文献5) 特開H7-200502 オムロン) トランザクション処理システムに関する二重化装置

インターネット(=the Internet)は非常に多数の計算機と計算機による網 以下、単に 網」とする)から構成され、これらはTCP／IPプロトコルを用いた通信リンクを通して世界的な規模で相互に接続されている。相互に接続された計算機は、電子メール、ゴーファー、およびワールドワイドウェブ等の、様々なインターネットサービスを利用して情報をやりとりしている。

インターネットは、網割当て団体から一意に割当てられたIPアドレスによって、そのホストを識別している。IPアドレスは、計算機が処理し易いように固定長の数字の羅列として表現されており、人間にとっては無意味綴りであり、覚えたり毎回間違えずに入力したりするのが困難である。TCP／IP網においては、ホストを特定する為には少なくともIPアドレスが必要であり、IPアドレスでホストを特定

することが人間にとって判りにくいものであるという問題を軽減する為に、ドメインネームシステム（以下、「DNS」とする）を用いてホストを特定することがおこなわれてきた。

DNSは、IPアドレスのような数字の羅列ではなく、人間にとって意味がある文字列でインターネット上のホストを特定するためのデータベースシステムである。階層的な名前空間を構成しており、ドメイン名と呼ばれる文字列を登録しておき、これをIPアドレスと対応づけることによって、インターネット上のホストを特定する。これを正引き名前解決という。逆に、IPアドレスからドメイン名を検索することを逆引き名前解決という。ＤＮＳの特徴は、ルートサーバを頂点とする木構造の分散データベースである。また、IPアドレスはルーティングの制約を受ける（すなわちIPアドレスは、IPアドレス体系の中での位置情報である）が、ＤＮＳにおける名前はホストの網的な位置とは無関係に存在できる。

一般にインターネットに常時接続し、IPアドレスの割当てを受けた各利用組織は、ドメイン名の登録団体に対して、ドメインの登録をおこない、自組織のためのドメイン名の運用をおこなう。この時にドメイン運用をおこなうサーバがＤＮＳサーバである。なお、ＤＮＳサーバの登録には、ドメイン名の登録団体に対してIPアドレスおよびホスト名を指定して、ＤＮＳサーバの登録をおこなう。

ルートサーバは第一レベルのＤＮＳサーバに、第一レベルのＤＮＳサーバは第二レベルのＤＮＳサーバに、そして最終的に上で示したIPアドレスの割当てを受けた各利用組織のＤＮＳサーバにドメイン運用の権限の委譲をおこなう。図１７に、ＤＮＳの検索順を示す。IPアドレスの割当てを受けた各利用組織のＤＮＳサーバでは、ドメイン名に対するホスト名とIPアドレスの対応づけや、メールの配送経路の指定等といった実際の設定をおこなう。

旧来ＤＮＳは設定ファイルを手動で設定および更新されてきた。ところが主に社内で利用されるプライベートLAN等において、Ｗｉｎｄｏｗｓ（登録商標、以下同様）パソコンの普及とダイナミック・ホスト・コンフィグレーション・プロトコル（ＤＨＣＰ）による端末となるパソコンの動的な網設定の普及によって、Ｗｉｎｄｏｗｓパソコンが再起動されるたびにIPアドレスが変化する等の、従来のように静的に１のホスト名と1のIPアドレスを対応づけることが難しくなってきた。ダイナミックＤＮＳとは、ＤＮＳサーバのレコードの更新をクライアントからのアップデート要求によって自動的に更新するしくみを提供するものである。ダイナミックＤＮＳの利用について、社内ＬＡＮ等の直接インターネットに接しない網における利用だけではなく、インターネットのグローバルサービスの中でも、現在、実用性の検証がされている。

インターネットのグローバルサービスの中でダイナミックＤＮＳサービスを利用した場合には、網割当て団体から網の割当てを受けないあるいはプロバイダから固定的なIPアドレス割当てを受けない（ダイヤルアップの）ホストで、インターネットサービスを提供することが出来るようになる。

ところで、ダイヤルアップとは、主にダイヤルアップ接続としてインターネットに接続する際に電話を

かける行為を伴うものをいうが、近年ケーブルテレビやデジタル加入者回線、光ファイバや衛星リンク等をアクセス回線に用いた定額制のIP接続役務等によるアクセス回線の多様化により、必ずしも電話をかける行為を必要としなくなっている。これら近年の常時接続型と呼ばれるインターネット接続役務は、単に接続時間による課金体系でなくなったことを意味し、ルータのセッション異常終了（停電等）、回線の異常、センタの故障やメンテナンス等により接続が異常切断された場合や接続業者もしくはダイヤルアップするホストの無通信タイマによって回線が切断された場合等に再接続すると、IPアドレスが変わる場合があるという点で専用線による接続と異なる。また、移動体通信端末の場合において、無線基地局を移動した場合等にIPアドレスが付け変わることがある。このような場合（すなわちハンドオーバした場合）にも、本明細書では便宜上、端末ノードのIPアドレスが変化するという点で、ダイヤルアップに含めることとする。

そこで本発明では、従来の専用線による接続に代表される網割当団体から恒常的な網の割当てを受けて接続する場合かプロバイダ（あるいはIPアドレスの割当てを受けた各利用組織）から恒常的なIPアドレスの割当てを受けて接続する場合と対比して、プロバイダ（あるいはIPアドレスの割当てを受けた各利用組織）からの一時的な利用を前提としたIPアドレスの割当てを受けて接続することを（モデムを用いて電話をかけるという行為を伴わず、DHCPやPPPoE等による割当てであったとしても）「ダイヤルアップ接続」といい、一時的なIPアドレスの割当てを受けるための動作をすることを「ダイヤルアップする」という。また、IPアドレスの一時的な割当てそのものを「ダイヤルアップ」ということとする。

ダイナミックDNS特有の問題

従来の技術では、IPアドレスが変化するホストでのインターネットサービスの提供はできなかったが、ごく最近になってダイナミックDNSを用いることによって、限定的に（グローバルサービスとしてのDNSは固定IPアドレスが必要なことからDNSを除く）インターネットサービスを提供できるようになった。しかし、ダイナミックDNSを用いることに特有の以下の問題点があった。これを以下、図01乃至図12にダイナミックDNS特有の問題の発生から収束までの過程を紙芝居形式で説明する。

図01。管理対象機器（以下、「T」とする）（100）からプロバイダ（以下、「P」とする）（000）へダイヤルアップ（PPPoE等を含む）する。

図02。T（100）はP（000）からIPアドレスの動的割当てを受ける。この時、割当てを受けたIPアドレスを仮に172.16.100.100とする。

図03。T（100）はダイナミックDNSサーバ（以下、「D」とする）（000）へDNSの更新要求をし、こ

れを受けてD (1000)は図02で説明したT (4100)に割当てられたIPアドレス(仮に 172.16.100.100)とT (4100)のホスト名を関連付けて設定する。

図04。T(4100)は、インターネットの一般利用者(以下、「S－2」とする)(5300)からのアクセスを受ける事ができる(正常状態)。

図05。なんらかの理由でT (4100)からP (4000)への接続が失われる等の障害が発生する。

図06。T(4100)からP (4000)へ再接続 (PPPoE等を含む)する。

図07。T(4100)はP (4000)からIPアドレスの動的割当てを受ける。IPアドレスが変化するまで割当てられていたIPアドレス(仮に172.16.100.100)とは別のIPアドレス(仮に172.16.200.10)が割当てられる。

図08。T(4100)はD (1000)への更新要求をし、D (1000)は図07で説明したT (4100)に割当てられたIPアドレス(仮に172.16.200.10) とT(4100)のホスト名を設定する。

図09。図07において、この時、T (4100)のIPアドレスはIPアドレスが変化するまで割当てられていたIPアドレスとは別のアドレス(仮に 172.16.200.10)を割当てられており、T (4100)にIPアドレスが変化するまで割当てられていたIPアドレス(仮に 172.16.100.100)は同一プロバイダの別のユーザT'(以下、「T'」とする) (4200)に割当てられている。この場合において、S－2 (5300)から見るとホストがすり替わっているかのように見える。

図10。インターネット全体では参照されるDNSはここでいうD (1000)ではあり得ず、利用者毎に直接接続されたプロバイダのDNS (4500や5500等)である。そのため、仮にD (1000)が正常に更新されたとしても、キャッシュの生存時間内には、利用者毎に直接接続されたプロバイダのDNS (4500や5500等)からD (1000)への名前問合せは行われない為に、これらのDNSサーバにT (4100)のIPアドレス(仮に172.16.200.10)が反映されるには時間がかかる。

DNS (4500や5500等)は、一度問合せをおこなったリソースレコードに関して、一定期間ローカルに記憶しておく。これをキャッシュという。キャッシュは、リソースレコードのTTL (=time to live)で指定された期間だけ記憶され、その後破棄される。これをキャッシュの生存時間という。DNS (4500や5500等)はキャッシュの生存時間中、リゾルバ(4100や4200あるいは5300等)からの問合せに対して、ローカルな記憶を参照して名前解決する。キャッシュは一度おこなった名前問合せを繰り返すことを抑制し、効率をよくする為に考えられた。しかしD (1000)においては、このキャッシュというメカニズムが逆にT (4100)のIPアドレスの変化に追従できない等のうまく合致していない部分があるので、以下に説明する。

図16に、S－2（300）からどのようにDNSが探索され、目的ホストであるT（100）に到達するかを順に見てみる。

①、S－2（300）からP－2のDNS（以下、「P－2－D」とする）（500）へ、T（100）について正引き名前問合せをおこなう。

②、P－2－D（500）は、まず、目的ドメイン名を知っているかどうかを調べ、知っている場合は、即座に目的ホストであるT（100）のIPアドレスをS－2（300）に返す。この時、P－2－D（500）が目的ドメイン名を知っている場合とは、目的ドメイン名をP－2－D（500）が運用している場合と、目的ホストであるT（100）に対するIPアドレスがP－2－D（500）に、キャッシュされている場合である。P－2－D（500）が目的ドメイン名を知らない場合を、図17に示す。

③、②によってT（100）のIPアドレスを知ることができたS－2（300）は、これをもとに、T（100）へアクセスする。

図17は、図16の②で、P－2－D（500）がT（100）のドメインを運用していない場合と、キャッシュされていない場合（最初の名前問合せの時）のDNSの探索順である。

①で、S－2（300）からP－2－D（500）へ、T（100）について正引き名前問合せをおこなう。

②、P－2－D（500）は、目的ドメイン名であるT（100）のドメインを運用しておらず、キャッシュの中からも見つけられなかった場合、Root DNSに、名前問合せをする。

③、Root DNSは、仮に目的ホストであるT（100）のドメイン名が例としてJPドメインであった場合には、JP DNSの所在を返す。（T（100）のドメイン名がJPドメインではない場合には、ccTLDなり、gTLDなりを管理するネームサーバの所在をP－2－D（500）に返す。）

④、P－2－D（500）は、③で得たJPドメインのDNSに対して、目的ドメイン名であるT（100）のドメイン名について名前問合せをする。

⑤、JPドメインのDNSは、目的ホストであるT（100）のドメイン名を運用するサーバ（ここではD（000））の所在を（JP配下のドメインは、JPNICおよび会員のサーバに登録されるツリー構造であり、第二レベル毎のDNSには分かれていないため、すぐに）P－2－D（500）にD（000）の所在を返す。

⑥、P－2－D（500）は、⑤で得たD（000）に対して、T（100）の名前をキーに、IPアドレスを正引き名前問合せをする。

⑦、D（000）は、T（100）の所在をP－2－D（500）に返す。

⑧、P－2－D（500）は、⑦で得たT（100）の所在をS－2（300）に返す。

⑨、S－２（300）は、Ｔ（100）へアクセスする。

図１８。DNS（500 や 5500 等）は、最初の名前問合せによってキャッシュされ、その後キャッシュの期限が過ぎた事によって、キャッシュが無効となるよう設定するのが一般的である。このキャッシュが無効なタイミング（図 17）では、Ｄ（000）に対して名前問合せがおこなわれる為に正しくＴ（100）のＩＰアドレスが得られる。しかし、キャッシュが有効な間（図 16）にＴ（100）のＩＰアドレスが変ってしまった場合、Ｄ（000）に対する名前問合せなしにキャッシュされたＩＰアドレスが返される為に、図０８での更新より以前の（キャッシュされた）ＩＰアドレス（仮に 172.16.100.100）が返される。なお、図１６の②のとおり、Ｓ－２（300）の接続先であるＰ－２－Ｄ（500）がＴ（100）のドメインを運用している場合には、キャッシュの問題は発生しない。

図１１。その為に、インターネット全体から見れば、キャッシュを参照するこのタイミングで、Ｔ’（200）がＴ（100）として誤認されてしまうおそれがある。

またこの時、Ｔ（100）はメールサーバやｗｗｗサーバの機能が設定されたホストであるものとしてもＴ’（200）はメールサーバやｗｗｗサーバの設定はされていないホストであるか、仮に設定されていたとしてもＴ（100）の設定とは違う内容である為に、Ｓ－２（300）からは、Ｔ（100）が正常でない状態（障害発生中）にあるように見えてしまう。

図１２。この問題は、インターネット上の各プロバイダのＤＮＳ（500 や 5500 等）が、キャッシュの生存時間が過ぎ、Ｄ（000）に再度、名前問合せをおこなえば、収束される問題である。その為に、時間が経過するにしたがって、図１２のような正常な状態となる。

次に、図０１乃至図０５および図１３乃至図１４に回線断後、Ｔ（100）が再接続しない（回線断のままの）場合について、時間の経過とともに正常に復帰する通常の場合（図０１乃至図１２）と同様に、紙芝居形式で説明する。

この場合に、考えられる理由は回線障害やダイヤルアップをする、あるいはダイナミックＤＮＳ更新する）プログラムの障害等である。

図０１乃至図０５までは、前述の説明と同じである。次に（図０６乃至図１２はキャッシュ問題の説明であるため、とばしていただきたい）、

図１３において、この時、Ｔ（100）はインターネットへ接続されていない状態のためＰ（000）は、Ｔ（100）にＩＰアドレスが変化するまで割当てられていたＩＰアドレス（仮に 172.16.100.100）をＴ’

4200)がダイヤルアップした時点で、T' 4200)に割当てる。

図14。D 1000)に設定されているT 4100)のIPアドレスは、更新そのものが出来ない為に、切断前のIPアドレス 仮に 172.16.100.100)が設定されている。その為に、やはりT' 4200)がT 4100)と誤認されてしまう。

ところで回線断は、T 4100)において検出可能なイベントであると同時に、外部環境の変化でもある。

表01は、T 4100)における、T 4100)の状態と割当てIPアドレスの関係からの障害のパターンである。

表01)

IPアドレスの状態 / T 4100)の状態		回線断前のIPアドレス≠再接続後のIPアドレス		回線断前のIPアドレス＝再接続後のIPアドレス
		回線断以前にTに割当てられていたIPアドレスを使っているホストが存在しない場合	回線断以前にTに割当てられていたIPアドレスを別のホスが使っている場合	回線断以前にTに割当てられていたIPアドレスが再度割当てられた
回線断のまま (パターン1)		アクセス不可	誤認 (図14参照)	—
DNSへの動的更新の失敗 (パターン2)		アクセス不可	誤認	OK
回線断後再接続 (パターン3)	キャッシュの生存時間内	[illegible]	誤認 (図11参照)	OK
	キャッシュされていない場合	OK	OK (図12参照)	

パターン1は、回線断のままの場合である。T 4100)が回線断後再接続出来なかった場合には、回

線断以前に割当てられていたIPアドレスがT'(200)に割当てられている場合に、誤認となる。割当てられていなかった場合に、アクセス不可となる。アクセス不可とは、目的ホストであるT(100)に到達せずに見失われた状態である。回線断のままの場合は、DNS(500や5500等)への再更新を、T(100)は当然することが出来ない。

パターン2は、DNSへのダイナミックアップデートに失敗した場合である。T(100)のダイナミックアップデートに係る部分のプログラム障害やD(1000)の障害等によって起こる。この場合において回線は、接続されているか、切断されても再接続されているものとする。この時の動作は、パターン1のT(100)が回線断後再接続出来なかった(回線断のまま)場合と同様に、回線断以前に割当てられていたIPアドレスがT'(200)に割当てられている場合に、誤認となる。割当てられていなかった場合に、アクセス不可となる。また、割当てIPアドレスが変化しなかった場合には、S－2(300)からの通信には問題がない為に、正常であるようかのようにみえる。

パターン3は、回線断後再接続した場合である。キャッシュの生存時間の影響を受け、網掛け部分はキャッシュの生存時間の影響を受ける部分であり、それ以外は、キャッシュされていない為に、名前問合せがうまく行っている場合である。ここでT(100)にアクセスしてくるS－2(300)は、インターネットの一般的な利用者であるため広域的に拡散して存在している。このとき、個別の各S－2(300)が以前に名前参照したことがあるか、あればキャッシュされている間の名前参照であったかによって、網掛け部分に含まれるか否かが決定される。

表01において、網掛け部分は、T(100)が回線断後再接続し、D(1000)への更新も成功している場合における、T(100)の動作としては正常であるにも関わらず、DNS(500や5500等)がT(100)のIPアドレスをキャッシュしている為に、T(100)が一時的に障害状態にあるように見えてしまうタイミングである。

以上に、キャッシュというメカニズムが逆にT(100)のIPアドレスの変化に追従できない等のうまく合致していない部分があることを説明してきた。

この問題はダイナミックDNSの仕組が旧来のDNSへの拡張であり、後付けされたものである為に、発生する。

前記した通り、旧来DNSは手動で設定および更新されていた。D(1000)を利用した場合には、T(100)からD(1000)への更新の間隔が短い場合に、D(1000)を参照(正引き)して得られたT(100)のIPアドレスは必ずしも正しいとは言えない場合があり得ることを説明してきた。

キャッシュの生存時間経過後、D(1000)へ名前問合せするタイミングに比して、T(100)の回線断

およびIPアドレス更新の間隔が短すぎると、S－2（300）は常にT'（200）をT（100）と誤認することになる。回線の不安定を原因とするこのような場合にも、DNSとしては機能することが望まれるが、D（000）としてはこの場合において、機能し得ず一種の障害状態とみなし得る。

これはDNSをめぐるインターネット全体の問題であり、個別の実装等によって（個々のホストが対応するだけでは）解決することができない問題である。

キャッシュ問題の実例

以下に、キャッシュ問題の実例を示す。

図19乃至図21にキャッシュの生存時間の為に、キャッシュされたDNS（500で計測）を参照する場合とD（000）から直接正引きした場合とで、T（100）のIPアドレスが違っている実例を示す。

図19に実際に計測した際のプログラムを示す。本プログラムはUNIXのシェルスクリプトである。行末の矢印（←>）は表示の都合上折り返されているだけで、本当は1行であることを示している。

図20乃至図21に計測結果を示す。各試行は、1行目が試行番号、2行目が試行した時間を示し、3行目がインターネットワーキングにおいて標準的なDNSの実装であるISC版BINDのdigコマンドがD（000）を参照した結果に文字列処理を施し、T（100）のIPアドレスを抽出したもの（a、c、e）であり、4行目から6行目までがpingコマンドがキャッシュされたDNSであるところのPのDNSサーバ（以下、「P－D」とする）（500）を参照した場合のT（100）のIPアドレス（b、d、f）である。（註：P－D（500）はT（100）が通常参照するところのDNSサーバである。ここではT（100）において試験した為にP－D（500）を参照したが、S－2（300）において試験する場合にはP－2－D（500）を参照するべきである。各端末において参照されるDNSは、リゾルバによって決定される）なお7行目から10行目は前記pingコマンドの付帯する出力である。

試行に用いたDNSサーバは、既にダイナミックDNSサービスを提供しているDynDNS.ORGをD（000）として用いた。試行時において、このサーバのキャッシュの生存時間の設定は1分である。なお、この1分という値はきわめて短い。

第1回目の試行と同時にT（100）からの更新要求を送信し、第1回目の試行と第2回目の試行の間に更新が完了している。そのため、第2回目の試行から前記digコマンドの出力（D（000）が示すT（100）のIPアドレス）とpingコマンドの出力（この試験ではP－D（500）を参照したが、P－D（500）はキャッシュの生存時間の影響を受ける）は、それぞれ、別のIPアドレスを示している（下線部a＝下線部bから下線部c≠下線部dへと変化）。

これが収束（下線部e＝下線部f）するのは、第16回目の試行である。この時、第16回目の試行は

第2回目の試行からちょうど1分後に試行されている。

このように、キャッシュの生存時間の影響により、どのＤＮＳを参照するかによってアドレスのずれが生じている。しかし時間の経過とともに収束している。Ｄ（1000）のキャッシュの生存時間は1分と短いが、それでもこのようなずれは生じる。

一般的な誤解

ところでここまでの説明に反して、ダイナミックＤＮＳ特有の問題はあまり一般には知られておらず、特許出願においてすら以下のような誤解がある。

例えば、特許文献３の段落0047において、「nslookupの回答が異常になる」とある。

しかし、これは異常にならない。

なぜならば、

1、nslookupした返事はエラーではない。特許文献３には、エラーでないにも係らず異常であると判断できる根拠は示されていない。

2、nslookup問合せに対してＤＮＳが返すものは、仮に、Ｔ（100）のプレゼンスが失われているとしても（またT'（200）が使用しているにしても）、最終更新されたIPアドレスである。（キャッシュされたIPアドレスである場合がある。問合せ先ＤＮＳに依存する。しかし、いずれの場合でも問題がある）

この場合、単純に異常であるとすることはできず、アプリケーション的な比較判断が必要である。すなわち、ここでＤＮＳが返すIPアドレスが異常であることを検出する為には、まず到達性確認等によって、ＤＮＳがポイントするIPアドレスがTそのもの（100）によって使用されているかTでないホストすなわちT'（200）によって使用されているかを判別することができて、はじめて異常かどうかがわかるのである。

Ｔ（100）による明示のオフライン処理があった場合も同じである。この場合は、T'（200）を生じさせないという効果はあるにせよ、やはりnslookupした返事はエラーではない為に、設定されたIPアドレスに対してアプリケーション的な比較判断が必要である。また、Ｔ（100）障害時や回線障害時には、オフライン処理等は一般にされないので、注意が必要である。

ここで仮にＳ－２（300）もしくは管理サーバ（以下、「S－1」とする）（2000）が、Ｔ（100）の従前のIPアドレスを記憶しておいた場合も、従前のIPアドレスとnslookupした返事としてのIPアドレスを比較すれば、IPアドレスの更新がされたことを知ることができる。しかし、それが現在の状態を反映しているかどうかについては、知る事ができない。この理由は、前記2による。キャッシュ問題の影響も受け

るが、この場合はT (100)がD (000)に対する更新処理ができない場合 例 回線断が継続している場合や更新プログラムの障害の場合等)には、D (000)がT (100)のIPアドレスとして返す値は、あてにならないことによる。つまり既にT (100)が使用していないIPアドレスを返すおそれがある。

ただし、特許文献3では、T (100)そのものが nslookup した返事を自ホスト(T (100) 特許文献3では分散サーバ3)のIPアドレスと比較しているようにも読み取れる。その場合は、nslookup した返事が異常であるとの判断は可能である。単に自ホストのIPアドレスとnslookup した結果を比較 ただし後述する接続形態1乃至3の場合のみ可能) しているためである。しかし、分散サーバ3を除くすべてのホストにとって、異常かどうかを知ることができない。すなわち分散サーバ3のみが知る事ができる。しかし分散サーバ3に相当するT (100)が自己に割当てられたIPアドレスを知ることができるのは、むしろ自明である。本発明ではS－2 (300)において、T (100)に正しく到達しているかどうかを確認できるようにすることがテーマである。

なお更にいえば、分散サーバ3は、わざわざnslookup するのではなく、単に自らに割当てられたIPアドレスの変化をトリガとしてIPアドレス更新依頼メールを動的DNSサーバへ送信した方が、妥当する。

また、特許文献3の段落0048において、例えば、 ICMP (Internet Control Message Protocol)の回答がなくなる」とある。

しかし、 回答がなくなる」とはいえない。この場合は不定である。

ICMPはICMPエコー要求のことだと思われる。これはコマンド実装に由来して、通常pingと呼ばれる。

タイミングの問題であるが、仮にT (100)が回線断に陥った直後に、P (000)がT (100)からでない接続要求を受ければ、直前までT (100)が割当てられていたIPアドレスを割当てられる可能性は高い。すると、T' (200)が出来上がる。するとpingは、T (100)は生きていることを示す。

よって、 回答がある」場合がある。

例えば、キャッシュ問題の実例の図20に示す試行回数2の場合である。図20中のcとdが異なった値を示すことに注目されたい。

試行回数1と試行回数2の間にT (100)は、図04の状態 正常)から図05 切断)、その後再接続して、図08の状態にいたっている。図09に示す別のユーザがダイヤルアップした場合に、T' (200)が出来上がる。T (100)がT' (200)にすり替わって、かつDNSを正引きしてもIPアドレスの変化がないためである。当然にT' (200)から「pingの回答がある」。タイミングさえうまく合えば、 pingの回

答は、途切れることなくT (200)に引き継がれるだろう。

そして、「pingの回答がある」からといって、T (100) 特許文献３では分散サーバ３が正常であるとはいえない。

前記の場合は、T (100)が復帰した時点でＤＮＳ更新する為に、キャッシュ問題を考慮しても、時間の経過に伴ってやがては収束される。しかし、最も問題となるのは、T (100)が図０５の状態のままであって、図０６以降の状態に移行する事ができなかった場合 障害）である。キャッシュの問題とは異なり、図１３で別のユーザがT' (200)に化けたが最後 図１４）、T (200)からのpingの回答を受取って、T (100)が正常だと判断し続けることになる。

以上から、

ビデオカメラによって、撮影された動く物体が仮に大きさまで判ったとしても、それが犬なのか人間の子供なのか、あるいはボールなのかは機械には識別できない。

しかし、この映像を人間が見れば上記のいずれであるかは、見た瞬間に判別できる。

同様に、nslookup や ping 等では、上記問題は解決され得ず、正常に見える 特許文献３では、これを異常であることが分かるとしている)。

これは、通信の相手方が、T (200)であった場合に、例えば、Ａさんのウェブページを見に行ったはずなのに、Ｂさんのウェブページが表示されれば、明らかに間違いであることが、人間には見た瞬間に判別できるが、機械にはそれが誤っていることが、分からないという問題である。

よって、到達性確認なしに、正しい到達性を有するT (100) と そしてTと誤認されたホストであるところのT' (200) との区別をつけることは、機械にはできない。

以上によって、一時的に動的なIPアドレスを割当てられたホストにおいては、ホストの動作としては正常であったとしても、障害状態に見えてしまう等の問題があり、ダイナミックＤＮＳの出現によって解決されたかに見える発呼すべき相手先識別は十分とはいえない状況にある。

ダイナミックDNS特有の問題点のまとめ

ここで、ダイナミックＤＮＳ特有の問題点をまとめてみる。

まとめ1。D (000)は、T (100)が接続されなくなった後も、最終更新されたリソースレコードをアナウンスし続ける。T (100)からの明示のオフライン処理等がされれば、存在しないT (100)に関する情報をD (000)がアナウンスし続けることはない。しかし、T (100)の障害時や回線断の際には、オフライン処理をすることができない。

まとめ2。T 4(100)のIPアドレスが変化した場合に、キャッシュの生存時間内は誤認される。

拡大された先行技術の範囲

ここまでは、ダイナミックDNSに関して、あて先端末を発見する過程における不備について見てきた。しかし同様の問題は、ダイナミックDNSのみに限らずおこりうる。例えば、特許文献1や特許文献2、ENUM等である。

このうち、ENUMに関しては、ダイナミックDNSの拡張であって、従来の電話網（PSTN）における電話番号体系をDNS上にマッピングするものである。

特許文献1は、ユーザ・ロケーション・サーバなる概念が附加されているが、ENUMと類似のものと考えてよい。

特許文献2は、DNSを用いずに、替りにホストを特定する静的な識別子と動的に割当てられた住所に対する特定のマッピング公示システムが提案されている。

ダイナミックDNS特有の問題点のまとめの1に挙げた「D 1(000)は、T 4(100)が接続されなくなった後も、最終更新されたリソースレコードをアナウンスし続ける」ことが、誤認を生じさせる原因であるので、特許文献1および特許文献2に関しては、これを解決する特定の方法を開示している。曰く、特許文献1では、端末側からDNSへキープアライブ信号を送信することによって、生存していることを通知している。特許文献2は、DNSを用いないながらも、DNS相当側からT相当側に向かってヘルスチェックを行い、T相当が接続されない状態になったことを検出している。

いずれの場合も、端末が網上に存在しなくなった場合に、マッピング公示システム上の該当するレコードを消し込むことによって、発信元端末がそもそもあて先端末を発見しないようにしている。

しかし、いずれの場合も、第三者端末SからのT (4100)への到達性の正しさ（エンドーエンドでのアクセス可能性）は、検証されない。

発明が解決しようとする課題）

S－2 5300)がT 4(100)だと認識していたとしても、実際には別の無関係なホストであり得る。そこで、T 4(100)だと認識されているホストとして本当に正しい通信相手であること、すなわち、T' 4200)に到達しているのでなく、あて先たるT 4(100)に対して正しく到達していることを確認する手段を提供する。

あわせて、前記到達性確認の結果をどのように利用するかについて、提案する。

発明の効果）

固定的なIPアドレスを与えられたTCP／IP網上のホストの管理は、通常であれば機器監視としてpingコマンド等を利用してホストの活死を監視することができる。しかし、ダイヤルアップのホストにあっては、そのIPアドレスが変化することから、pingによる管理では、誤った（T 4100）でない）ホストがpingに応えていても、正常に稼動していることになってしまう。本発明では、T 4100）が正しい到達性を有するホストであることを確認するようにして、これまで管理することのできなかったIPアドレスの変化するホストを、管理できるようにした。また、通常の管理をおこなう場合にも、従来であればIPアドレスが変化するホストは管理することができなかったが、通常の管理の前段の処理として本発明を用いることによって、その後のより高度な管理（例えば、CPU負荷やトラフィックの監視）をも可能とした。

概要）

T 4100）だと認識されている通信相手に本当に正しく到達していることを確認する手段は、以下の方法で以って確認する。ここではS－1 2000）からT 4100）に対して通信をした結果から、T 4100）が正しい到達性を有するホストであるかどうかの判定を、S－1 2000）がする。

課題を解決するための手段は、以下の２の段階による、外部的なホスト間通信の過程によっておこなう。

第一の段階はアドレス確認であり、

第二の段階はサイン・アンド・カウンターサインである。

図23に、第一の段階および第二の段階によって、S－1 2000）がT 4100）の到達性確認をおこなう場合の動作を示す。

アドレス確認は、第一の段階であって到達性確認のためのパラメータの対のうちの一を形成する（後述する通信モデルを参照）。

S202において、S－1 2000）からキャッシュの生存時間の問題を避ける為に、D 1000）に対して名前問合せ（正引き）をする。

S204において、S 202の返事からT 4100）のIPアドレスを得る。

なお、T 4100）のIPアドレスの確認は、S－1 2000）とD 1000）が同一のホストである場合かS－1 2000）のリゾルバがD 1000）を向いている場合や、D 1000）のTTL（キャッシュの生存時間）の設定が極めて短い場合等は、省略することができる。

また、D (000)には冗長化された場合があるが、ここでは単に冗長化されたサーバ群を以って、単一のサーバと同じだと考えて差し支えない。

サイン・アンド・カウンターサインは、第二の段階である。

アドレス確認が省略できる場合があることから、狭義の到達性確認でもある。

S202およびS 204でT (100)のIPアドレスが得られたこの時点では、T (100)が正しく認識されたとおりのT (100)であるかどうかは、未だ確認されていない。T (100) とP (000)間の回線断やD (000)に対してT (100)が更新することができない場合等では、到達性確認の過程を通じて、Tだと思われたホストが正しい到達性を有していないことが初めて判明する。また、T (100)において提供されているサービスがあらかじめわかっていたとして、このサービスに正常にアクセスできない場合も、キャッシュの影響と言い切ることはできず、単にそれだけでT (100)が網から断たれた状態にあるとは、判断できない。例えば、T (100)がP (000)に正常に接続されておりかつD (000)への更新も正常にされている場合であって、かつキャッシュの問題も発生していない場合であってなお、サービスを提供するプログラムに障害がある場合が考えられるからである。網管理的な考え方としては、T (100)がインターフェース障害や回線断等の網的な障害 根本的な障害)に陥っているのか、あるいはサービス障害 アプリケーションレベルの障害)なのかを切分けたいところである。ここで、障害切分けは低レイヤからするのが定石である。そこでこの時点では、とりあえずT (100)だと思われるホストに対して通信を試み、その結果から本当にT (100)なのかどうかを判別することによって、まず網的な障害の有無を確認することとする 詳しくは後述する設計思想を参照されたい。ここでは、とりあえずT (100)のインターフェースまで到達できるかどうかを確認したい)。

S206において、S－1 (000)からアドレス確認S２０２およびS２０４の結果から求められたT (100)のIPアドレスに対して、あらかじめ合意された方式での通信 これを「サイン」という)をおこなう。

S208において、S206の返事 (この返事の内容を「答えるべき返事」といい、この返事を運搬するものを「カウンターサイン」という)の有無を判断し、返事があればその返事をS 210に受渡し、返事がなければT (100)が見失われている旨を表示するS216へ進む。

S210において、S２０６の返事を受取り、この返事に対して、文字列処理をして、不要な文字列を取除いた文字列を求める。

S212において、S208で抽出された文字列と、S－1 (000)に記憶されたあらかじめ合意された方式での通信に対してT (100)からの答えられるべき返事とを比較する。

ここで、T (100)が答えるべき返事とS－1 (000)が受取るべき返事は同じ物であることが合意され

ている。

あらかじめ合意された方式での通信に対する答えられるべき返事と一致した場合は、T (100)は正しい到達性を有している。

一致しない場合は、キャッシュの生存時間の問題とは無関係に、T (100)はインターネットに接続されていないか何らかの問題でセンタ側ＤＮＳに対する更新が出来ない状態にある、との判定をおこなう。

判定の結果を表示する。S212の判定によって、T (100)が正常稼動しかつ正しい到達性を有するT (100)であることが確認された場合Ｓ２１４か、あるいは障害状態であることが確認された場合Ｓ２１６かに分けられる。この判定結果を受けてどうするかは、T (100)の運用責任者と到達性を確認する者との契約に基づくべきものであるため、ここでは単に結果の表示とする。T (100)が正常稼動しかつ到達性が正しい場合Ｓ２１４では、従来は監視不可能であったIPアドレスが変化するホストに対して、トラフィック監視等の通常の監視に後続させることができる。一般的には、Ｓ２１４の場合には正常である旨のみをログに書出す等してあえて通知せず、T (100)が正常でない状態の場合Ｓ２１６は、アラートをあげる等の状態を通知する処理に進むのがよい。S216の場合、T (100)がD (000)を更新したタイミングと重なった場合等に、D (000)が更新を反映するのに遅延が生じる可能性を考慮して、やや時間をおいて再度本プロセスを実行しそれでも障害が検出されるのを待った後、初めてアラートをあげるのか、あるいは誰にどのような方法でアラートをあげるのかを考慮するとよい。

カウンターサインの本質

次に、到達性確認とは、何かについて述べる。例えばT (100)において公開されているウェブページを見た場合、人間であれば、それがＡさんのウェブページであるのかＢさんのウェブページであるのかは、容易に識別がつく。分かり易くいえば、Ａさんのウェブページを見に行ったはずが、Ｂさんのウェブページが表示されれば、T (200)であり（もちろんＢさんのウェブページが表示されるのではなく、単にタイムアウトするまで待たされた挙句、エラーになった場合でも同じ）、Ａさんのウェブページが表示されれば、相手先は正しい到達性を有するＡさんのウェブページである。このように人間が見れば即座に判別できる。ところが、前記した通り、機械にはそれを識別することができない。これを機械（＝通信ノード）にも識別できるようにすることをいう。

到達性確認の結果は、真偽で表される。結果が真の場合とは、正しい到達性を有する場合である。真性のホスト等と表現されることもある。結果が偽の場合とは、正しい到達性を有しない場合である。

では、ここで仮にT (100)が固定的なIPアドレスを割当てられていた場合はどうであろうか？

1、前記同様、ウェブページの例のように、もちろん人間が見ればわかる。いわゆる人間による目視確認である。

仮に見てわからなくても、調べればわかる。このとき、大体次のようなことを調べる。

2、nsbokupでもわかる。pingでもわかる。

3、ホストそのものが名乗るので、わかる。ただし、ここでホストが名乗るとは、サービスと呼ばれる通信プログラム（以下、この通信プログラムを「Daemon」と呼ぶこととする）を経由して、名乗ることとする。また、従来は、ここで名乗った返事を聞いた通信の相手方が、それに基づいて特別なアクションを起こすことはなかった。ここで特別なアクションとは、例えばそれによって接続の許可拒否を判断する等である。

4、アカウントがあれば、パスワード認証を利用することもできる。

さて、本発明の前提であるT（100）がダイヤルアップのホストである場合に戻るとしよう。

1については、到達性確認の目的は人間だけでなく機械にもわかるようにすることなので、ここでは考慮しない。

2のnslookupは、既に説明した通り、本当に正しい相手先かどうかが不明なままである。pingも同じである。

4は、サーバにおけるアカウントの問題である。本発明は相手先サーバ あるいはホストにアカウントがあることを前提としていない。そのため、アカウントがあることを前提としての認証については、別論である。

さて、では、3はどうであろうか？

Daemonは通信ポートを開けて接続を待つ常駐型のプロセスのことであるが、だいたいホスト名、プログラム名、バージョン名等を名乗るものである。

よって、3は使うことができる。

これは、T（100）が固定IPアドレスの場合には、当然に通信の開始時点において、行なっていたことである（ただしこれを元に通信をするかしないかを判断することは、従来はされていない）。

ここでホスト名に対するアクセスに対して、Daemonが名乗るということは、単に自己の識別情報を示しているに過ぎない。

これは認証という概念には含まれないものである。

そして、単に名乗るだけで到達性確認はできる。

すなわち、到達性確認とは、

サインとして、「Who are you?」とたずね、

答えるべき返事として、「私は誰某です」と答えさえすればよいのだ。

よってカウンターサインの本質とは、当然に名乗るべき自己の識別情報を名乗るためのキャリアである。

そしてサインとは、T（100）に名乗らせる為にどのように尋ねるかという取決めである。

ここで、ダイナミックＤＮＳ亦は静的な識別子と動的な住所が関連付けられることがある程度普及したことによって、初めて気付かされた、網の新たな特性について説明する。

静的な識別子と動的な住所の関連付けにおける一方向性

D（000）で利用できるのは、一般に正引き名前解決のみである。

逆引き名前解決をした場合には、IPアドレスに対して、ダイナミックアップデートされるべきホスト名を返さない。

では、何を返すか？

一般にIPアドレス割当を受けた当該アドレスブロック（ＣＩＤＲブロックを含む）の網を運営する網運営主体の設定したホスト名を返す。この表現はわかりにくいかも知れない。代表例としてインターネット接続業者（←Internet Service Provider。以下、「ISP」とする。ISPはP（000）の一形態である）のホスト名が挙げられる。

以下に例を示す。

正引き host.customer.co.jp —> 192.168.0.99

逆引き 192.168.0.99 —> ppp000099.otemachi.provider.com

正引き ppp000099.otemachi.provider.com —> 192.168.0.99

となって、host.customer.co.jpは隔絶されている。すなわち、ppp000099.otemachi.provider.comが誤認されたホストである場合に、ppp000099.otemachi.provider.com は、host.customer.co.jp というホスト名を知ることができない。

ここで、

host.customer.co.jpは、T（100）がD（000）に対して更新するホスト名、

192.168.0.99は、T（100）がその時点で割当てられているIPアドレス、

ppp000099.otemachi.provider.com は、前記 IPアドレスに対して逆引きして得られるホスト名であって、ISPが名前を付けたものである。

この理由は、以下のとおりである。

委任（＝DNS delegation）DNS Reverse Delegation に関連するものとして、RFC2050、2317、3152等がある）の前提に反するので、つまり、管理権限の問題として、他人（他の組織）が管理する網への逆引きを設定することができないということである。例えば、D（000）の所属する網と、P（000）の網が異なる組織によって運営管理される場合において、D（000）はP（000）に対する逆引きを設定することができない。

ところが、host.customer.co.jp は、S－2（300）からアクセスを受付ける為に、T（100）の所有者が、広くアナウンスするものである。

すなわち、このhost.customer.co.jp なるホスト名は正引きの際に使用される周知のキーワードでありながら、逆引きでは知ることができないという特徴を有する。

T（200）がサインを受付けとった場合には、静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる網の特性から、発信元があて先として何というホスト名を指定していたかを知ることはできない。

偽装

ただし、そうでない場合がある。例えば、あて先ポートが HTTP の場合等は、セション確立時にはホスト名は当然に含まれないが、その後のＧＥＴ命令等にあて先（閲覧者が見たいと思っている）ホスト名が含まれる場合がある。そのような場合には、ＧＥＴ命令以下に含まれるホスト名を抽出し、オウム返しにするプログラムを誤認されるおそれのあるホストに実装すれば、答えるべき返事、そしてこれをキャリーするカウンターサインを偽装できる。これは、受動的攻撃である。

偽装された場合の影響範囲

しかし、現実的ではない。なぜならば、

偽装しようとする場合には、誤認されたホストT'（200）へのアクセスをひたすら待つ必要があり、

仮にこのような偽装が成功したとしても、T（100）の割当 IPアドレスが次に変化したタイミングで、追従することができなくなるからである。

このことから、T（100）の割当 IPアドレスが変化しない間を限度として、偽装が成立する。

そのため、D（000）への更新処理をのっとらない限りは、あまり効果がない 偽装できたとしても、

長くは続かない）ことになる。すなわち更新処理をのっとった場合のみ、完全にそして誤認なく偽装することができる。ただしこの場合は、既に偽装ではない。

そして、カウンターサインは更新の際に用いられるパスワードとは、関係がない。

よって、D（000）への更新処理は守る必要のある通信である。

偽装される場合はこんなとき

まず、誤認が発生する必要がある。誤認されたホストT'（200）でなければ、偽装することができない。

偽装したホストT'（200）は、サインを受取った際にTを名乗る 答えるべき返事」をキャリーするカウンターサインを返すことによって偽装する。

ここで、T'（200）はT（100）と同様にP（000）からIPアドレスを割当てられる。そして、T'（200）のIPアドレスはT（100）と同様に変化し得るものである。このことから、以下のことがいえる。

T'（200）は、T（100）と同様にP（000）配下のアドレス範囲に属する。すなわち誤認され得る範囲はあらかじめP（000）のIPアドレス範囲によって制限されている。しかし、この制限は、網のありようから決定されるものであって、なんら人為的な制限ではない。

T'（200）は、T（100）と同様にP（000）から一時的に割当てを受けた住所であるところのIPアドレスを使い続けることができない。そのため、仮に偽装された場合であっても、偽装したホストT'（200）は、いつまでも偽装し続けることができない。

偽装が成立する場合は以下の通りである。

基本的には、キャッシュの問題を除けば、T（100）が障害状態に陥った場合にのみ偽装可能である。その上で、偽装が成立する期間は以下の通りである。

T'（200）のIPアドレスが変わらないあいだ

T（100）が復帰して、再度更新するまでのあいだ

以上のことから、前記偽装される場合はありうるが、しかし影響範囲は許容されるものとして扱う。

ただし、サインとして あなたは誰？」といった単に応答をうながすのが推奨されるのであって、 あなたは誰某ですか？」のように偽装し易い状況を作るサインは、推奨されない。誰某の部分には、具体的な名前等が入るものとする。

到達性確認独立の効果

到達性確認と更新の乗っ取りについて比較してみた。以上から、到達性確認は守る必要がないと

いえる。

到達性確認と更新とは、直接の関係を有しない独立した過程である。

そして、到達性確認はアカウントに対するパスワードといったものではない。

これが、到達性確認独立の効果である。

理論）

1、通信モデル

登場人物一覧

まず、本発明において特別な意味を持つ「値」を示す。

A 動的な住所（＝network address）

網のための値であって、端末への実際の到達性を司る住所

Pから一時的に割当てられる

B:静的な識別子

ヒトのための値であって、あて先端末を特定するための識別子

次に、機能を示す。

D :マッピング公示システム

発信元が通信を開始しようとする時に、静的な識別子と動的な住所を対応づけて参照させることによって、あて先端末への到達性を発信元に提供する

Tに替わって、組A：Bを公示するもの

T:あて先端末

本モデルにおいてあて先となる端末

Dに対して組A：Bが関連することを設定するものである

計算機である必要はなく、通信ノードでありさえすればよい

S:発信元端末

Tをあて先とする場合の、Tへの到達性の正しさを確認する端末

Tに対して、到達性の正しさを確認する

計算機である必要はなく、通信ノードでありさえすればよい

P：Tに対して、一時的な住所であるところのAを割当てる機能

一般に網の場合と特定のサーバの場合がある。

電話会社的な考え方をすれば、Tを内包する網そのものである。電話会社の例でいえば、DCEはクロックを出す側、DTEはクロックを受ける側と考えられる。すなわちクロックは網そのものから受ける。これを援用して、例えばインターネット接続に係るISPの場合は、IPアドレスを割当てるものは、ネットワーク・アクセス・サーバ（例 Livingston Portmaster や Ascend MAX等のこと）やRADIUSサーバではなく、ISPの網そのものが割当てるものと考えられる）

LAN的な考え方をすれば、DHCPサーバ等がこれにあたる。

ここで、AとBからなる組を「組A：B」と表現する。

組A：Bの実像

Tにおいて、BはT自らを示すことを公にするための識別子である。そして、Aは、Pから一時的に割当てられた住所である。ここで、Bのみでは、Tから見た第三者であるところのSからは、網的な到達性を有するものではない。Aのみでは、網的な到達性は有しているものの、Aは一時的にTがPから借受けて使用する住所であり、また、T以外の端末も利用するものであるから、第三者からはTとAを結び付けることができない。しかしながら、Bは本来的にTを指し示すべく公示された情報であり、また、この時点において、Aはまさしく Tに割当てられている住所である。この事実を以って、Tは組A：Bの実体（以下、「実像」とする）を有するものとする。

組A：Bの写像

マッピング公示システムDは、Tによって組A：Bが対応づけられたものであることを通知され、記憶し、第三者Sからの問合せに応答して、組A：Bが対応づけられたものであることを問合せをする者に対して公示する。具体的には、AもしくはBのいずれかについて問い合せを受けると、BもしくはAのいずれか問合せを受けなかった方を応答するものである。また、別の観点からはAもしくはBのいずれかを入力とする場合に、組A：Bの残る一方を出力するシステムともみなせる。ここで特徴的なのは、Tは公示することができないので、DがTに替わって公示するということである。

このことから、Dにおいて公示されるのは、組A：Bの写像である。

ところで、誤った到達性を持つ場合に、よくTが誤っていてDが正しい等とされるが、これは正しくない。

すなわち、DにおいてマッピングされるAとBの組が実状を反映していなければ、SはTに到達する

ことができない。

実状とは、Tにおける組A：Bの実像である。

AとBからなる組は、それぞれ個別に正しいとか誤っているということができないものであって、AとBからなる組となって、そして、正しく実状を反映して、はじめてSはTに到達する事ができる。

逆に言えば、SからTに対して正しく到達しない場合には、組A：Bの実像を有するところのTが正しく、組A：Bの写像を公告するDが誤っているというものでも、その逆でもない。すなわちいずれかが正しく、いずれかが誤っているという類のものではなく、両者が一致していることが重要なのである。

ここで、両者とは、Dが記憶するTに関する情報の写像と、Tが保持するBとTがPから与えられたその時点での被アクセス条件であるところのAからなる情報の実像、すなわち組A：Bの実像と写像である。

以下、単に実像あるいは写像とする場合であっても、「組A：Bの」が省略されているものとする。

ここで、図22を参照されたい。

①乃至 ⑤は、順序だった過程である。

①において、TからDに対して、組A：Bが写像される。

②および ③によって、DS間の組A：Bが検査される。

④および ⑤によって、TS間の組A：Bが検査される。

以下、単に ①乃至 ⑤のいずれかを示したときは、図22における ものとする。

ここで、再度強調したいのは、Dにおける組A：Bの写像と、Tにおける組A：Bの実像が一致していなければ、第三者SはTに到達することができないということである。

この理由は、組A：Bの実像がTであることは疑う余地のないことであるが、TやDから見て第三者であるところのSはそもそもTを直接参照することができず、それゆえSはDの組A：Bの写像を参照することによって、Tに対する到達性を得ている。

すなわち、Tは実像をDのみに写像するものであって、第三者であるところのSからTが参照されることはない。

この理由は、Tは第三者Sから見てあて先にあたるので、Tを発見する為にまずDを参照するのであるから、Tが発見できない時点でTを参照することはできない。

SからTへのアクセスが可能になるのは、SがTを発見した後の話である。

よって、以下のようにすれば、発信元Sがあて先Tに正しく到達することが検証される。

②および ③によって、検査されたDS間の組A：B（すなわち、組A：Bの実体の写像）と

④および ⑤によって、検査されたTS間の組A：B（すなわち、組A：Bの実体の実像）とが、一致すれば、発信元Sからあて先Tへの到達性は正しい。

2、シーケンス

ではどのようにして、組A：Bの実像と写像が一致しているか否かを判定するのだろうか？

これには、シーケンスにおとして考えてみる必要がある。

再び図22を参照されたい。

値AおよびBの関係をシーケンスで説明する。

① TがDに、組A：Bの写像を作成する。

② SはDに対して、Bで以って問合せる。

③ DはSに対して、Aを応答する。

④ SはTに対して、 ③で得られたAを用いて（Tであろうと思われるあて先に）問合せる。

⑤ TはSに対して、Bを応答する。（Tであろうと思われたあて先が、実は）Tでなかった場合には、不明な応答となる。ここでTが応答しない場合は、応答がないという応答があったものとする。これも不明な応答に含める。つまり0という値はない訳ではなく、存在するとの考え方に基づく。以下、本明細書はこのような抽象化に基づいて記載される。

各シーケンスの内容を説明する。

①は、Tが組A：Bの実像を、Dに写像する過程である。この結果、出来上がるものがDにおける組A：Bの写像である。この際、適当な第三者が適当なTに対する嘘の組A：Bを写像できないようにする為に、通常はTD間では認証過程を要する。

なお、後に詳述するが、組A：Bの実像は、T単体の場合のみでなく実施例8に詳述するTと一体となった装置を含めた集合である場合がある。また、写像する主体は、DHCPサーバやISP等の場合（やオペレータENUM）等のPがする場合がある。

②および ③は、一連の手続きとしてセットで考える。一般的な表現でいうところの名前問合せに相当する。

②において、Dが組A：Bのうちいずれかを入力すると残る一方を出力するシステムであることを利用して、Sは、周知のキーワードであるところの静的な識別子BをDに名前問合せをする。

③では、 ②の結果として ①で設定されたDにおける組A：Bの写像から、残る片方であるところの動的な住所であるところのAを応答する。

ここまでの ①乃至 ③の動作については、従来技術である。ここでは、 ②および ③の動作をセットで、利用すべき自然現象（外部オブジェクト）として捉える。

④において、Sは、 ③で得られたTに対する到達性を有するはずのAをあて先として、単に何らかの応答をすることをうながす。Aは ③から ④にいたる過程で、一時的に利用されるものであるので、単に代入されるだけでよくSでは別段記憶する必要がない。 ただし、記憶した方がよい場合があるので、これを考察に説明する）

⑤は、組A：Bのうち、残る方すなわちBを応答する。応答されたもの、すなわちSがTから受け取った返事がBであるならば、 ②でした最初の問合せと ⑤の返事がオウム返しの関係にあるので、正しくTに到達していることになる。なお、 ④でされた 何かを応答しろという要求に対して、Tが不明な応答をする場合と峻別される。

これによってSは、

②および ③の過程から、組A：Bの写像を、

④および ⑤の過程から、組A：Bの実像を、

知ることができる。

上記シーケンスの後、Sは、 ②および ③の過程で得られた組A：Bの写像と ④および ⑤の過程で得られた組A：Bの実像について、一致しているか否かを比較する。

なお、以下にタイミングについて説明する。

①の実像から写像をコピーする動作は、Sから見てあずかり知らぬ動作であり、そのタイミングについては、知ることができない。

②および ③の、組A：Bの写像を得る過程は、Sにとっては能動的な振舞いであるので、任意のタイミングで実行できる。

同様に、 ④および ⑤の組A：Bの実体を問合せる過程も、任意である。これは、Sが欲したタイミングでも良いし、また、Sの内部タイマに基づいても良い。そして、この ④および ⑤の動作は、必ずしも ②および ③の直後である必要はない。

例えば、いったん到達性が確認された後の（2回目以降の）到達性確認においては、 ④でするサインのあて先であるところのTの住所を記憶しておき、通常は ②および ③の過程を省略し、SからTに到達しなくなった時点、すなわち到達性の正しさが確認されなくなった後に、再度 ②および ③

の過程を実行しても良い。

②及び ③、そして ④及び ⑤の過程は、要求と応答の関係にある。

また、特に ⑤の過程において、 ⑤は動作であると同時に、 ⑤は Bのキャリアであって、バケツと水の関係にある。

3、拡張

ところで、写像同士を比較する場合であっても、前記理論は適用できる。

ただし、Dが既にプライマリ・セカンダリあるいはマスタ・スレーブ等のモデルによって、冗長化されている場合は、その冗長化されているグループ内で写像同士の比較判定をおこなったのでは、不十分であるので注意されたい。すなわちこの場合は、 ②および ③のみを2度試行し、これを比較しているにほかならないのであって、これでは本来的に比較にならない。

したがって、写像同士を比較する場合は、本来的に無関係なマッピング公示システムに対して、Tが別々に写像している場合に有効である。すなわちDに相当するマッピング公示システムが、冗長化されない異なるDが2系統以上ある場合である。しかし、このような条件を付せば、対応できるTは多いとは言えないはずである。そのため、別の方法を考える。

この場合の方法は、 ④および ⑤の過程で、 SはやはりTに対して通信を試みるのだが、特に ⑤の過程で、Tが応答するものにB以外を用いる方法である。

この方法は、Sにおいて、Tと関連付けられて記憶された文字列を、 ⑤においてTはBの替りに応答すれば良い。したがって、この場合の ⑤においてTが応答する文字列の内容は、Tと関連付けられていることをSが知っている限りにおいて、あらゆる文字列が使用可能である。

同様に、TS間で合意されたなんらかのルールに基づいて、あらゆる文字列を更に変形された場合をも許容されるべきである。すなわちBの代替は、置換の場合だけでなく、変形の場合であってもよい。

あらゆる文字列とBそのものの関係は微妙である。

一方であらゆる文字列は、Bの拡張であり、Bからの派生である。

他方、あらゆる文字列であるということは、Bを単に文字列と見た場合には、当然にあらゆる文字列はBをも含むものである。

このようにいずれが上位概念であるかは、微妙なところである。本明細書では、あらゆる文字列はB

の代替物であるとする。この際、あらゆる文字列を成立させる為には、Tと関連付けられていることをSが知っているとの条件付きではあるが、この条件については、以降いちいち条件付きである旨を書かずに省略することとする。

⑤において、TがSに対して応答する文字列の内容について、整理してみる。

Bそのものの場合は、Sは、あて先としてのTの静的な識別子Bのみを、知っていれば良い。

あらゆる文字列の場合は、Tを示す静的な識別子に加えて、Tと関連付けられた文字列もしくは変形ルールを、知っている必要がある。

以降の記載では、単にBとした場合はBの代替物を含むものとし、Bそのものあるいは Bの代替物のいずれであるかが重要な場合のみ、Bそのもの、Bの代替物とあえて記載するものとする。また、Bの代替物の中で特に置換の場合と変形の場合を区別する必要がない限り 単に Bの代替物あるいはあらゆる文字列と記載することとする。

なお、Sにおいて ②の過程でBを以って問合せることから、 ⑤でBそのものが応答された時には、略してオウム返しの関係と記載することがある。この場合は、あきらかにBそのものであって、Bの代替物を含むことはない。

ここまでが、本発明を実施するための通信モデルである。

以下に、機能を実際につかさどる具体的な装置を示す。具体的な装置がいずれの装置であるかについては、網の状況や位置関係等から複数の装置がありうる。これら特定の機能を実現する具体的な装置は、代替可能なものであって、その範囲において、特定の集合を形作る。

D:マッピング公示システム

Dは、本来的に冗長化されたサーバ群を構成する場合が多いので、このグループ内では、代替関係がある。典型的には、ダイナミックDNSやENUM DNS、そして特許文献1や特許文献2に開示されたBとAとのマッピングを公示するものである。

T:あて先端末

TがLAN内にあり、ゲートウェイについで公衆の蓄積交換網を経由して、DやSと通信する場合には、Pから見たエッジノードと一体となったものの間で、代替関係がある。この際の役割分担の実際については、実施例8に詳述する。

S:発信元端末

S－2の場合とS－1の場合がある。 基本的にSは、S－1とS－2のいずれであってもよい。そして、S－1とS－2とを明確に分けて考えなければならない場合は、クライアント・サーバ型で動作するときのみである。クライアント・サーバ型で動作するときのS－2は、到達性確認する機能を有しない場合がある）

本発明の実施にあたって、クライアント・サーバ・モデルを採用し、S－2がS－1に問合せ、S－1がS－2に替わってあて先への到達性を確認する場合は、S－1が発信元となる。

例外的にSは、Dと一体となっている場合がある。

P：Tに対して、一時的な住所であるところのAを割当てるものものである。

TがＬＡＮ上にあって、PがＤＨＣＰサーバの場合は、通常はＤＨＣＰサーバである。しかし、これはDやSをも、同一のＬＡＮかＬＡＮ間接続によって到達できる場合の考え方である。DやSと通信する為に、公衆網を経由しなければならない場合は、ISP等の網をPとするべきである。逆に言えば、PはTに対して一時的な住所であるところのAを割当てるのではなく、単にエッジノードに対して、Aを割当てている すなわち、Tに対してでない場合がある）。そしてこの場合のTは既に説明したように、ゲートウェイたるエッジノードと一体となって、参照されるノードである。これも実施例8に詳述する。

これらの位置関係および具体的なPやTが何であるかは、網の構成 接続のされ具合）によって、いずれかの具体的な装置が代替物の中から選択されるべきである。

以下に、動作について名前をつける。

(1) この過程は、TからSへ、組A：Bを写像する過程である。従来の技術であって、ＤＮＳの場合は 更新」動作にあたる。

(2) ＤＮＳの例では、 名前問合せ」である。用語の統一の為に、DがＤＮＳでない場合も 名前問合せ」とする。

(3) ＤＮＳの例では、 名前解決」である。やはり同様に、DがＤＮＳでない場合も 名前解決」とする。

(2)と(3)はセットである為に、片方の表現で残る一方の存在を暗示するものとする。

(4) 従来は到達性を確認するための過程は存在せず、ウェブアクセス等の通常の通信がこれにあたる。 サイン」と呼ぶこととする。 あらかじめ合意された方式での通信」ともいう。

(5) サインに対する応答であるので、 カウンターサイン」と呼ぶこととする。

(2)乃至 (5)による一連のシーケンスによって、組A：Bの実像と写像が得られる。こうして得られた実像と写像を比較することによって、到達性を判断するのが、到達性確認である。

④乃至⑤の過程では、置換亦は変形しても同様の比較をすることができる。そのため、答えるべき返事に用いることのできる文字列は、あらゆる文字列である。

さて、①乃至③の過程は、従来からされていることであることを既に説明した。

④については、それが一般的なアクセスである場合は、そのアクセス方法に応じた応答をTはする。

しかしそれゆえに、⑤においては、TはBを応答したり、あるいはSとのあいだで合意されたあらゆる文字列を応答したりはしないものである。

よって、⑤については特別に考慮して何らかの流用をするか、新たに実装しなければ、前記理論を用いることができない。

⑤の過程を担う者

以下、⑤の過程を担う者がどのように振舞うべきかについて説明する。ここでは答えるべき返事にはBそのものを名乗るものとして、例示する。

1、標準状態ではT（100）は名乗らないか、もしくは関係ない名前を名乗る。ここで関係ない名前を名乗るとは、例えばパソコンの場合には、あらかじめ適当な名前（ここで適当な名前とは、少なくともT（100）がドメイン名まで含めて、D（000）に対して動的更新するホスト名が設定されることは、よほど意図的にやらない限りはありえない）がついているので、それを名乗るということである。

2、しかし、これでは答えるべき返事として使うことは出来ず、適切な名前を名乗っているとはいえない。

3、したがってT（100）は、答えるべき返事として使用する名前を名乗らなければならない。答えるべき返事として使用する名前とは、D（000）において動的更新されるホスト名を指す。1から、これは明示的な設定変更を意味する。なぜならば、S－1（2000）はT（100）のドメインを管理するD（000）を参照して、T（100）のIPアドレスを得るわけであるが、この際の名前問合せに用いるキーであるところのホスト名を、T（100）からはオウム返しにしてほしいからである。

4、上記設定は特別な設定であって、普通はT（100）はこのように（3のこと）なっていない。

このような設定をあえてすることが、本発明のサイン・アンド・カウンターサインを成立させる上で必要なことである。

答えるべき返事が、Bの代替物である場合にも、同じ考え方でよい。

以上について、整理してみる。

到達性確認は、組A：Bの実像と写像を比較することによって成立する。この為には、組A：Bの実像と写像に関する4つの要素（値）を得る必要がある。そしてこの内、実像におけるBを示す値のみが、唯一従来からある方法では入手できなかった。そこで「カウンターサイン」というキャリアを提案した。キャリアは明らかに信号であって、情報を運ぶモノの意味である。

「答えるべき返事」とは、「カウンターサイン」によってキャリーされるものであり情報である。前記したBそのものであるとか、Bの代替物であるとかは、この情報の類型に当たる。「カウンターサイン」がバケツで、「答えるべき返事」が水である。「答えられるべき返事」とは、Sにおいて記憶される、「答えるべき返事」と対応付けられた情報である。⑤の過程において「カウンターサイン」によってキャリーされた、Tが「答えるべき返事」を受け取ったSが、Sにおいて内部的に記憶した「答えられるべき返事」と比較し、一致したかどうかによって到達性が正しいか誤っているかを、判断するものである。

前記⑤の過程を担う者では、流用として説明した。実施例1乃至実施例7に示す通信の方式は、従来技術である。しかし通信の方式を従来とは異なる使い方をすることによって、到達性確認という新たな価値を生み出すことができる。通信の方式とは、すなわちどの通信ポートを用いるかに過ぎない。したがって新規であろうと流用であろうと、いずれにしても通信ポートの範囲内に収めるしかない。そのため本来的には、新規のポートであることが望ましいが、これに関しては特許とは別の手続による標準化を待つべきである。流用とした理由は単純で、通信ポートに依存せずに、実施できることを明らかにしたかったからである。

ホスト名に何を名乗るかは、通常はT（100）の記憶装置に保存される。そして、Sからの通信要求（⇐サイン）に対して、Tが応答する（⇐カウンターサイン）際に読み出された後、応答に埋め込まれて返信されるものである。この返信の内容を答えるべき返事と呼ぶ。

そのためT（100）は、D（000）に更新するホスト名を名乗るように、明示的に設定されることが必要である。

しかし、置換もしくは変形されたものであっても、Bそのものと同様であるとしている。以下の答えるべき返事の類型で以って、この説明に替える。

答えるべき返事の類型

ここでカウンターサインによってキャリーされるTが答えるべき返事に用いることのできる文字列を類型してみる。DNSを例として挙げる。

1、ホスト名

Bそのものの場合である。ホスト名はFQDNであるものと仮定する。

あて先ホスト名＝返事のホスト名の場合を、理想的とする。しかし、ホスト名のみを返す場合はむしろ少なく、現実にはかなり冗長な返事が返されるものと思われる。

よって、当然に返事の中から答えるべき返事を抽出し、判断する必要がある。

すなわち、この場合はサイン・アンド・カウンターサインの典型にあたり、T 4(100)が答えるべき返事として使用するホスト名を名乗るようにする明示の設定変更との前記条件が満たされている場合は、単にオウム返しですむ為に、S－1 2(000)における答えられるべき返事の設定は省略可能である。アルゴリズムについては実施例1で、設定内容については実施例1および表02で説明する。

すなわち ②の過程でSからD 1(000)に問合わせられる内容がBであるのに対して、 ③および ④の過程を経て ⑤の答えるべき返事の内容もBである場合である。

Sにおいて、Bを二度記憶する必要はない。あて先と答えるべき返事が同じ場合 すなわちBそのもの)は、答えるべき返事を省略できる。

答えるべき返事は、複数であってもよい。

ところで、マッピング公示システムがDNSでない場合には、FQDNではなく静的な識別子そのものであると考えればよい。例えばFQDNを、特許文献2の場合には、ハンドル名と読替えればよい。

2、URIスキーム (=uri_scheme)

ホスト名を含むが冗長である場合が多ければ、いっそプロトコル名を含んでしまおうという考え方である。

プロトコル名を含むことによって、単一のホストで異なるサービスを提供している場合に、複数のホスト名の各々と関連付けられたサービスで待ち受けしても、各々のホスト名とサービスの対を別個に到達性確認できるのでよい。すなわち、単一のホスト上で別名（ドメイン違いを含む）のホスト名でサービスを提供する場合である。

唯一性がある。S－1 2(000)における答えられるべき返事の設定は、場合によっては省略可能である。

例として、user01.customer.co.jp という単一のホストで、以下のサービスを提供しそれぞれに到達性確認する場合を挙げる。

http://wwwhost01.customer.co.jp

mailto:sales@customer.co.jp

mailto:info-fax@faxsvr.customer.co.jp

sip:info@customer.co.jp

h323:info@customer.co.jp

h323:info-fax@customer.co.jp

tel:81-3-1234-5678

enum:8.7.6.5.4.3.2.1.3.1.8.e164.arpa

等である。

URI(Uniform Rsource Identifier, RFC2396)は、永続的であいまい性なしに参照できるという特徴を持つ。ここでは、URLはURIの特化されたフォームであるものとして取扱い、URIはURL(RFC1738)を含むものとする。本発明では、URIはホスト名を含むという点で、ホスト名の拡張亦はホスト名の延長上に位置する概念として取扱う。

この際、T(100)で待受けする到達性確認用のポートは、ウェルノウンであってもよいが、サービス用でない到達性確認専用のポートを別途ウェルノウンでないポートとして用意してもよい。

ITU-T E.164勧告に規定される国際公衆電気通信番号(以下、「電話番号」とする)を逆順電話番号.e164.arpaというホスト名(FQDN)に変形し、ダイナミックDNSへの入力とする(RFC3263)ことによって、既存の電話網との接続をはかろうとするものが、通称ENUMである。この際、RFC3403で文字列変形される際に発信人が受取人として指定する電話番号(RFC2916)も、答えるべき返事として用いることが出来る。この場合は、1に示した「あて先ホスト名=返事のホスト名」の場合と同様に、「最初と最後が同じ」でオウム返しの関係ならば到達性確認できるという点で、理想的である(電話番号あるいは前記変形された後の電話番号ホスト名の場合は、本来的には前記1のホスト名の場合に含まれる)。もちろん、前記変形の中間過程において得られるURIも答えるべき返事として用いることができる。

電話番号は、もちろん静的な識別子である。ENUMにおける、逆順電話番号.e164.arpaは、ホスト名であると同時に電話番号そのもの(異論はあるかもしれないが、単にDNS上にマッピングしただけであって、等価なので、電話番号そのものとした。すなわち単に表記法の違いである)でもある。電話番号そのものの場合は、答えるべき返事の類型において、URIではなくホスト名の場合に含めた方がよい。

すなわち、名前問合せの結果得られた最終文字列(←T(100)の正引き名前問合せ>サインを送

る相手としてのIPアドレス−>サインとしての問合せ−>答えるべき返事としての文字列)は、もちろんT(100)と結び付けられたものだが、T(100)は自らの自己の識別情報を示すものを答えるべき返事として返しさえすれば到達性確認できる。

ところで、URI形式を用いる場合には、T(100)のみならず、T(100)のユーザ(ヒト)を識別することも可能である。当業者であるならば容易に想到することができるが、実施例1に開示するアルゴリズム中での文字列処理部分を多段にするだけでよい。

すなわち、答えるべき返事には附加情報を含めることができる。

また、答えるべき返事は、複数であってもよいことから、一台のT(100)は、複数のサービス、複数の別名を各々到達性確認させることができる。

URIスキームの場合は、Bそのものである場合と、Bの代替物である場合との、境界線上に位置する。

URIスキーム中にBそのものが含まれる場合は、1ホスト名の場合に示したように、冗長な返事の中からT(100)が答えるべき返事を抽出するのであるから、1の場合と同じでBそのものだとみなせる。

しかし、URIスキーム中にBそのものが含まれない場合や、Bそのものでなく URIスキーム全体を合意した場合には、Bの代替物だと考えるべきである。

3、返事のホスト名が足りない場合。

Bの代替物の場合である。

ここまでは、ホスト名＝FQDNであることを仮定して、説明してきた。

ところが、FQDNでないホスト名を返す実装は存在する。

FQDNでないホスト名は、答えるべき返事からT(100)を特定できない場合である。

以下の3パターンが考えうる。

ドメイン名のみであって、狭義のホスト名が存在しない場合。

この場合はやや特別である。ドメイン名をカスタマが専用する場合は、FQDNと同じに扱ってよい。ドメイン名をカスタマが専用しない場合は、識別性がない(自己の識別情報として十分でない)。

狭義のホスト名のみであって、サブドメイン名、ドメイン名を含まない(非修飾シングルラベルの)場合。

ホスト名＋サブドメイン名であって、ドメイン名を含まない（非修飾マルチラベルの）場合。

名前検索する場合と異なり、S－1（2000）がT（100）の到達性確認の為にサフィックスを追加したりすることはない。

ホスト名がUSER01とかHOST01等の場合は、（Bにとっても）識別性がない。むろん、一意性はない。

しかし、これはこれでよい。

一意性がない為にS－1（2000）が受取った、T（100）が答えるべき返事から、T（100）を特定することができないだけである。

その他、S－1（2000）に登録されている文字列であって、ホスト名でもURIスキームでもない文字列も、Bの代替物である。

X509証明書や単にT（100）の公開かぎでもよいこととし、必ずしもホスト名をベースにする必要がない。すなわちホスト名でなくても、T（100）は自己の識別情報を名乗りさえすればよい。更に言えば、この識別情報はTS間において合意されていれば足る。ここでいうTS間の合意は、単にT（100）が勝手に決めて公衆にアナウンスした文字列である場合を含む。そのためFQDNやURIの場合と異なり、グローバルに一意である必要がない。

そして、T（100）の識別情報は当然にS－1（2000）は知っている必要があり、S－1（2000）はS－1（2000）内にあらかじめ保存されたT（100）の識別情報（←答えられるべき返事）と、T（100）であろうと思われる装置（通信の相手方）からの返事（←答えるべき返事）を比較することによって、到達性確認する。

以上、返事のホスト名が足りない場合そしてその他の文字列が、Bそのものの置換の場合である。置換の場合には、置換えられた後の文字列を直接TS間で合意する。それゆえ、置換の場合は静的である。変形の場合とは、変形ルールを合意するものである。それゆえ変形の場合とは、動的な置換にほかならない。

それゆえ、カウンターサインはSにT（100）の到達性を確認させるように機能する信号である。

答えるべき返事の特徴

偽装の項で既に説明したように、答えるべき返事はパスワードではない。すなわち、セキュリティ上の脅威たり得ない。よって、秘密にする必要がない。

従来からされてきた個体識別によって、T（100）を識別しようとするものではない。網の特性から得られる値を比較することによって、到達性が判断されるものである。

更に、Sは特定の一の通信ノードではない。SとしてS－2（6300）が挙げられているように、不特定多数である一般利用者をも想定されている。この場合は、秘密にする必要がないのではなく、実は答えるべき返事を秘密にすることができない場合である。この際に、Bの代替物を用いる場合には、T（4100）を示す静的な識別子だけでなく、置換え後の文字列や変形ルールをも事前にSに対して知らせておく必要がある。こう書くと現実的でないように思われるかもしれない。しかし、そうではない。例えば、ドメイン名のみでなく、URLとメールアドレスをセットで知らせることは、普通にされていることである。この例と同じだと考えれば、別段T（4100）側そしてS側における負担が増すわけではない。

しかし、別の場合もある。例えば、特定のS－1（2000）のみにBの代替物を知らせて、これを答えるべき返事に用いる場合には、実質的に秘密である。しかし、だからといって何らかのパスワードと混同すべきではない。本発明の柔軟に実施をすることができることを表すのみである。

以上から、S－1（2000）に記憶された（期待された）返事を含む文字列をT（4100）が返しさえすれば、到達性確認は可能である。

ところで、DNSは、リゾルバからは以下のように定義づけられる

（従来）

リゾルバからの問合せに対して

静的な識別子を

静的なIPアドレスに変形して出力するシステム。

（最近）

リゾルバからの問合せに対して

静的な識別子（ホスト名、電話番号）を

動的な識別子（URI）に変形し

多段の再帰クエリ（中間処理）を用いて

静的なあるいは動的なIPアドレスに変形して出力するシステム。

なお、最近の場合は従来のものを含む。

このように、DNSの位置付けが変化してきている。

この時、DNSが識別子を変形する過程は、以下のようになる。

別名（⇐CNAME） －＞ ホスト名 －＞ IPアドレス

電話番号 －＞ ホスト名 －＞ URI －＞ IPアドレス

答えるべき返事は、上記のうち、

IPアドレスを除く、

ＤＮＳへの最初の入力である静的な識別子の、あるいはＤＮＳでの識別子変形過程上で得られる（中間過程の）識別子の、

いずれであってもよい。

なお、上記のうち、別名で始まるものは、特別な意味を持つ場合がある。

第一に、別名によって、別のＤＮＳ上のホストを参照させることは従来からされてきたことである。すなわち、再帰性はＥＮＵＭ以前からあった。

第二に、その別のＤＮＳ上でポイントされたＴ（100）が動的更新される場合である。文字列変形を無視して単に動作として考えたとき、ＥＮＵＭと同じ動作ということができる。

ここでカウンターサインを複数返してもよいものとすると、エンド・エンドの場合のみならず、名前検索過程における中間過程のホスト（この場合はＤＮＳ）に対しても、到達性を確認することができる。Ｓでは複数返された答えるべき返事の中から、目的たる答えるべき返事を抽出すればよい。

この際、１のカウンターサインの中で、複数の答えるべき返事を返す方法と、カウンターサインによってキャリーされる答えるべき返事は１のみに固定し、複数のカウンターサインを返す方法とがある。

このように、複数のカウンターサインを返すことは、概ね2つのことに貢献する。

1つは、単一のＴ（100）において、複数の識別を可能とすること。

もう1つは、名前変形過程上の中間段階におけるノードがカウンターサインを複数返すことによって、追跡性を増すことが可能となること。この際、Ｔ（100）では、中間ノードがした応答の中から、お目当てのＴ（100）を示す答えられるべき返事を抽出するようにすればよい。こうすることによってtraceroute のように、中間ノードの到達性を確認することができ、障害時の障害個所の特定に多いに役立てることができる。

設計思想

網管理とは

ここで念の為に網管理の必要性について説明する。まず、用語の説明として、網管理自体は、いわゆる構成管理や課金管理等をも含む通常の管理の概念であって、その対象を網としているものであ

る。次に、管理と監視の関係は、網管理という大カテゴリの中で、ホストや網そのもの（例えば、トラフィック（＝流量）は個別のノードに対してだけでなく、全体に対しても計測できる）の監視という具体的な手法があるものと解されたい。網の状態は常に変動している為に、その状態を監視することが障害対応の第一であり、また、網設計へのフィードバックや将来の拡張計画の根拠資料となるべきものである。

しかし本発明では、T（100）は動的IPアドレス割当てを受けたカスタマ網の境界ノードあるいは境界ノードと一体となって参照されるホストであり、きわめて小規模なものである。しかし、何らかのTCP／IPサービスを提供するのであるから、回線断やシステム障害等によって、サービス提供ができなくなっているにもかかわらず気づかずにいたのでは、問題がある。そこで、なんらかの障害が発生した場合に、すみやかに通知され復旧すべきと考えて、このような小規模な網においても網管理は必要なものであるとして、従来管理することのできなかったIPアドレスが変化するホストにおいても管理できるようにしようというものである。

pingの意味

pingは、ICMPプロトコルのエコー要求を実装したプログラムとして、従来はホストの到達性（活死）確認に用いられてきた。

pingは、魚群探知機のごときものであって、はね返ってくれば、魚群（もしくはホスト）がそこに居ることがわかるというものである。

ところがこのpingは、IPアドレスが変化するホストをあて先とする場合には、仮にT（100）でなくT'（200）からpingの返事があった場合であっても、正しく相手先のホストが応答していることを示してしまう。しかしこの場合は、ホストへの到達性が確認できたとはいえない。

pingでは通信の相手方が本物かどうかがわからないので、本発明では「あなたは誰」とたずね、「私は誰某」と名乗った返事を聞いて、この返事が想定していた名前と合致していれば、T（100）がそこに居ることがわかるとしている。

本発明は、（従来のホストとは異なる）IPアドレスが変化するホストに対しては使用をすることができなくなった「ping」を代替するものとして、設計した。すなわちpingを全面的に代替することは目的としておらず（事実pingで実装される多くの機能を本発明では実装していない）、pingで到達性を知る事ができない場面ではじめて本発明をpingに代替して用いるものである。

そこで、本発明の理解を助ける為に、いわゆるping代替としての使用をする場合（S－２（300）がT（100）の到達性を確認する手段として本発明を用いる場合）のイメージを、図３９にしめす。（詳しくは実際的応用に示す）

なおここでは、T（100）の到達性を確認が出来ている場合とは、正しく通信の相手方に到達し反射が返されている場合であり、ping本来の目的である到達性確認に相当する。よって、到達性確認はpingを代替しうる。なお、pingの出力に含まれる経路周回時間（round trip time）等については考慮していないが、本発明の実装に経路周回時間の計算を附加することは、当業者であれば容易である。ただし、実際的応用に示す本発明をフィルタとして用いる場合には、経路周回時間等といった冗長な出力は望ましくないことを、実装上の注意点として挙げておく。

pingが相手先からはね返ってくる過程において、途中経路にいかなる網の雲が存在していようとも、あるいは網の雲を経由せずに単に同一のイーサネット上にあったとしても、これを意識しないのと同様に、本発明でも意識する必要はない（すなわち、エンド・エンドの通信である）。

設計上留意したこと

蓄積交換型の網が、本来持つ自律性を生かすことを目指した。

そして単純かつ明快であることを心掛けた。この単純さについては、後の時代にあってこれは自明であるといわれる程度の単純さによって構成される理念を目指した。

その他には、適用可能性が高いこと、可用性が高いこと、柔軟で規模に依存しないこと等を目指した。

実施可能性について。

従来技術を捨てることに対する人々の心理的な抵抗は大きい。

社会のインフラを変えなければ実施できないような発明は実際問題として、実施可能性は低いといえよう。よって、従来の技術を変更する要なく、附加することによって、利便性有用性を提供できるような実施の仕方が望ましい。

その意味で本発明は、スモールスタートでき、かつ規模に依存せず実施できるという点、そして従来の技術との高い整合を図り、従来技術を何一つ捨てずに実施できるという点で、普及の可能性は高いといえよう。

適用の範囲

本発明においては、IPv4およびIPv6で利用可能である。

動作モデルとしては、ピア・トゥ・ピア型でもクライアント・サーバ型でも動作する。

また、IPアドレスの携帯性および移動性の双方に適用可能である。

ここで、IPアドレスの携帯性とは、ノートパソコンの電源を一度切って、移動して（出張先のホテルや訪問先の会社）から再び電源を入れて使用する場合等をいう。

そして、IPアドレスの移動性とは、（移動体端末等において）通信を維持したままで、IPアドレスが動的にハンドオーバした場合等をいう。

IPアドレスの移動性について、混同されやすいものに、モバイルIP（＝IP Mobility、RFC2002乃至2006）がある。

まず目的が異なる。モバイルIPは自ら発呼した通信の返事をロストせずに受信することを目指す技術であって、少なくとも発呼側端末に被呼側（であるモバイル）端末の識別性を提供することは主たる目的ではない。

さらに、モバイルIPでは、動的な住所と静的な住所を関連付けるという点で、本発明とは考え方が異なる。その意味では、前記IPアドレスの移動性としたのは適切ではなく、住所の移動にかかわらず、本発明は静的な識別子と動的な住所の対を検証するものである。

実装について

本発明はアプリケーション層で動作し、トランスポート層には依存しない。ただし前記アプリケーション層は、ＯＳＩ（＝Open System Interconnection。ISOおよびＩＴＵ－Ｔによる標準）でいうところのセション層、プレゼンテーション層、アプリケーション層を含むものとする。このことから理解されるように、本明細書は連綿と続くＵＮＩＸ的な標準に従って記載されるものであって、ＯＳ等のその他の標準に従う場合は、その旨明記されるものとする。また、前記アプリケーション層で動作するとしたことは制限でなく、本発明が後にICMP等のネットワーク層で動作するプロトコルに代替されるものとして提案された場合にも、この場合は本発明の最初の実装がアプリケーション層で動作したものであったに過ぎず、本発明の思想の範囲内であるものとする。

実装）

以下、本発明の実装を図面に基づいて説明する。なお、各図面において同様の機能を有する箇所には同一の符号を付している。以下に掲げる実施例は、制限でなく例である。

実施例ではＳ－１（2000）として説明したが、Ｓ－２（6300）と置換てもよい。ダイナミックDNSを例に説明するが、既に説明したように、ENUMや特許文献1や特許文献2の場合でも適用可能である。

実施例1乃至実施例7は、サインの仕方として、どのような通信を用いることができるかを例示した。サインの仕方のことを、あらかじめ合意された通信の方式と表現する。この際、通信ポートに関しては通常そのポートを使用するプロトコルに従うものとする。実施例1乃至実施例7は、通信ポートについては、既存の（ウェルノウンな）ポートを流用して説明した。

実施例1の中で、前提となる考え方とアルゴリズムについて示す。

実施例1および実施例2は、T(100)＝網境界（＝エッジノード）の場合。典型的には端末そのものの場合。

実施例3および実施例4は、T(100)が網接続機器である場合、典型的にはＮＡＴＢＯＸの場合。

実施例5乃至実施例7は、T(100)がどのような機器であるかを問わない場合を示す。

実施例8の中で、網の構成と位置について示す。

実施例9の中で、新規の実装であるところの、例えばＮＡＴＢＯＸ等の装置への本発明の実装例を示す。

実施例10の中で、端末そのものであって、典型的にはモバイル端末の場合の実装例を示す。

実施例1

実施例1は、あらかじめ合意された通信の方式に、ＳＮＭＰを用いるものである。

T(100)は計算機であり、直接ダイヤルアップ接続している。ＳＮＭＰエージェントを実装しており、通常の正しい設定がされているものとする。実施例8で詳説する図37の接続形態1である。

S－1(2000)では、監視プログラムをタイマ実行している。

S－1(2000)において、

1、インターネットではUNIX（登録商標、以下同様）サーバが非常に多く使われているため、本発明実施の場合にも、UNIX上で動作させる場合が多いだろうことが想定されること。

2、UNIXにはウェルノウンポート等で待受けする主要なインターネットサービスがあらかじめ導入されているか、少ない費用と労力で導入することができること。

3、UNIXには文字列処理環境が最初からＯＳの一部として提供されていること。

等によって、本発明部分のみの実装で実験環境が構築できることから、ＵＮＩＸ上で実験した。

Windows系のＯＳの場合は、ＤＮＳについてはISC版BIND（最初のＤＮＳの実装としてバークレー版ＵＮＩＸに採用されて以来、インターネットの標準ＤＮＳである）に入替える。あるいはISC版BINDの代替物に入替える。代替物とは、ISC版BINDに含まれるdigコマンドのようにＤＮＳサーバの情

報を外部から精査できるものをいう。ＳＮＭＰマネージャについては、マイクロソフト社製のものを用いてもよいし、ＯｐｅｎＶｉｅｗ（登録商標、以下同様）等の製品を新たに導入してもよい。文字列処理環境については、Ｗｉｎｄｏｗｓ系のＯＳにあっては十分にはＯＳに含まれていないので別途文字列処理環境を用意するか、本発明を実装する際のプログラム開発中に組み込みとした方がよいかもしれない（ただしこの場合、ＩＳＣ版ＢＩＮＤに含まれるｄｉｇコマンドの出力に対するプログラムインターフェースの問題もあるので、いっそｄｉｇコマンド代替から作成してしまった方が、労力が少ないかもしれない）。

Ｔ（100）においてＰＣが使われる場合には、Ｗｉｎｄｏｗｓ系のＯＳの場合は、ＷｉｎｄｏｗｓＮＴやＷｉｎｄｏｗｓ２０００にはＳＮＭＰエージェントが含まれている為に、そのまま利用することができる。

以上によって、ＯＳの種類に関わらずに、本発明を実施可能である。

ＳＮＭＰ等の通信の方式は、待受け側のポート番号として、以下特にことわりのない場合は、ＲＦＣ１７００ ＡＳＳＩＧＮＥＤ ＮＵＭＢＥＲＳ に規定されたウェルノウン・ポートと同じか類似のものとする。ＲＦＣは、ＡＲＰＡＮＥＴ開発時代に、通信の方式を合意する（よりよくする）為に 意見を求む（＝Ｒｅｑｕｅｓｔ Ｆｏｒ Ｃｏｍｍｅｎｔｓ）」として公開された文書を起源とし、現在ではインターネットあるいはＴＣＰ／ＩＰによる通信における標準的な規約集として機能している。

ＳＮＭＰ（＝Ｓｉｍｐｌｅ Ｎｅｔｗｏｒｋ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ）は、けして単純とはいえない標準的な網管理用のプロトコルである。ＳＮＭＰにおける通信ではコミュニティ名およびＴ（100）の到達性確認で用いるべきオブジェクトＩＤを通信の方式として合意し、Ｔ（100）に設定されるオブジェクトＩＤの値を答えられるべき返事として合意する。例としてコミュニティ名に初期値のままのＰＵＢＬＩＣとし、オブジェクトＩＤにホスト名を意味する ｓｙｓＮａｍｅを用いる。

ｓｙｓＮａｍｅはＳＮＭＰエージェントの設定上、ほとんどの場合で明示的に設定するものではなく、単にシステムのホスト名をそのまま引用する。ここでは、「⑤の過程を担う者」における明示の設定変更および 答えるべき返事の類型」に従うものとする。Ｔ（100）に設定されたホスト名は、Ｄ（1000）に登録される完全修飾ドメイン名（Ｆｕｌｌｙ Ｑｕａｌｉｆｉｅｄ Ｄｏｍａｉｎ Ｎａｍｅ。ホスト名＋サブドメイン名＋ドメイン名からなる。以下、「ＦＱＤＮ」とする）が設定されているものとする。ごく一部の装置ではＦＱＤＮを設定できずドメイン名を含まないホスト名のみ設定できる場合がある。この場合であって、あえてＢそのものを答えるべき返事の値に用いたい場合には、実施例２を参照されたい。この場合は、Ｂの代替物を答えるべき返事の値に用いた方が単純である。

ここでオブジェクトＩＤは、返事の内容（＝識別子）が代入される変数だと考えればよいので、以下の

ようになる。

オブジェクトID（sysName）の値＝FQDN＝返事の内容＝T（100）のホスト名。

S－1（2000）に登録されたT（100）名や返されるべき返事等の通信の設定に必要な項目を、表02に示す。

表02）

	S－1(2000) or S－2(5300)		向き	T(4100)	
設定項目	あて先たるTを示す静的な識別子	(値)			
	サインの仕方	(あて先通信ポート)	サイン －＞	サインの受け方	(受け側通信ポート)
	答えられるべき返事	(値)	＜－ カウンターサイン	答えるべき返事	(値)
	├ Bそのものの場合	Tを代入すればよいため、設定不要		├ Bそのものの場合	Bそのもの
	├ Bの置換の場合	置換え後の文字列		├ Bの置換の場合	置換え後の文字列
	└ Bの変形の場合	変形ルール		└ Bの変形の場合	変形ルール

表02から判るように、Sにおいてあて先たるT（100）を示す静的な識別子が追加される他は、STともに共通である。T（100）が答えるべき返事が、Bそのものである場合には、S側においてのみその設定を省略することができる。

Sにおいては、カウンターサインを受取る事によって、通信モデルにおけるシーケンスを完成させる。この後、SではSの内部に記憶されていた答えられるべき返事を読出し、カウンターサインによってキャリーされたT（100）からの答えるべき返事と比較する。そして受取った返事（Bが答えるべき返事）と内部記憶した答えられるべき返事とを比較した結果の真偽によって、T（100）に対して正しい到達性を有するか否かを峻別するのである。なお、返事を受取った際に、受取った返事を一時記憶する変数が必要であるが、これについては計算機工学上自明でもあり、また、この変数そのものは本発明においてさして重要でない為に、単に受取るべき返事とする。

S－1（2000）においては、到達性の確認に必要な項目を設定する場合は、シーケンシャルファイルのレコードとして記憶装置に保存してもよいし、DBMSを通じてアクセスされるデータベースであっても、かまわない。また、T（100）毎にプログラムを用意し、そのプログラム中に設定情報を記述する

方法でもよい。これらはS－1（2000）において管理するT（4100）のボリュームに応じて選択すればよい。プログラム中に直接埋め込む方式は、T（4100）の数が多くとも数百等の比較的少ない場合によい選択である。ここで設定される内容は、T（4100）あたりに必要な項目が含まれていればよく、附加情報が追加されていてもよい。附加情報の例として、T（4100）の使用するドメイン名を運用するD（1000）の住所等が考えられる。特許文献2に適用する場合には、IPアドレス情報通知サーバの住所を記憶する。また、項目が並ぶ順序についても表02の通りでなくても、T（4100）あたりとして混乱のないように保存されるようにすればよい。

本発明では、記憶装置については、レジスタやキャッシュについては考慮せず、メモリおよび外部記憶装置を指すこととする。また、外部記憶装置は、S－1（2000）やT（4100）の当該機器内に内蔵されるローカルな装置である必要はないものとする。例えばハードディスクドライブにおいて、ファイバーチャネル等を経由してアクセスされるディスクアレイであっても、NFSマウント等をされるような共有型のディスクであっても、単にハードディスクドライブとして扱う。一時記憶は、機器の再起動等の際には保持される必要がないものであり、比較的短時間で消去されるものであるが、一時記憶はメモリ上に展開されても、ハードディスクドライブ等に一時ファイルとして展開されてもよい。

T（4100）においては、通信の設定に必要な項目は多くない。これらは、合意された方式での通信要求に応答するプログラム部分と返事そのものであるところの通信の設定に必要な項目すなわち、パラメータからなる。プログラムが実装済みであるならば、保存すべきデータ量が少ないこととなる。これらの通信の設定に必要な項目を保存する記憶装置には以下のものが考えられる。機器内の不揮発メモリ、CFカード・スマートカード等のメモリカード類、PCMCIAインタフェースを有したハードディスクドライブか通常のハードディスクドライブ、ディスケットドライブ、MOドライブ、テープ装置等の記憶装置 か、DVD－RAMやパケットライト方式のCD－RWもしくはイメージを作成するものとしてCD－R等の取り外し可能な記憶媒体を利用した記憶媒体読取り装置）が利用可能であるし、書換えの頻度が極めて低い場合が考えられることから、当該機器において直接に記憶媒体に対する書換えをするのではなく交換によって保存内容の修正をおこなうCD－ROM、DVD－ROM、ROMカートリッジ等の取り外し可能な記憶媒体を利用した記憶装置まで可能である。ところで、USBインターフェースやIEEE1394インターフェースの記憶装置であっても、ハードディスクドライブにおいてSCSIインターフェースなのかIDEインターフェースなのかを区別する必要がないのと同様に、インターフェースの種類については区別する必要がない。その他にも、例えば、システムの起動時にあらかじめ指定されたホストからTFTP等の通信を用いて、設定をロードすることも可能である。この場合の記憶装置は通信を経由した外部のホストであり、内部の記憶装置に一時記憶させることによって用

いる。

これらは、実施しようとする環境（具体的な装置）にあわせて利用可能なものの中から選択すればよいものとする。

ところで、図15に示すように、T（100）の使用するドメイン名を運用するD（000）に対して、名前問い合せをしなければならない。すなわち、D（000）は基本的に複数あるのが前提であり、問合せ毎に問合せ先であるD（000）を切り替えることになる。例えば、T1（101）の使用するドメイン名を運用するDNSがD1（001）であり、T2（102）の使用するドメイン名を運用するDNSがD2（002）である場合等は、S－1（000）の動作としてそれぞれ異なるDであるところのD1（001）とD2（002）とを切り替えて、名前問合せをする。もちろん、ここに図示しないT3（103）の使用するドメインを運用するDNSがD1（001）である場合には、T1（101）およびT3（103）の名前問合せを、D1（001）に対してまとめた方が良い。

よって、以下に示すアルゴリズムは、T（100）毎亦はD（000）毎に、毎回するものである。

図23にアルゴリズムを示す。

アドレス確認

S202およびS204はアドレス確認である。これにより、キャッシュの生存時間の問題を解決している。

キャッシュの生存時間の問題とは、DNSサーバ（500や5500等）からT（100）のIPアドレスを正引き名前問合せをしようとする時に、D（000）の指定したキャッシュの生存時間中の2度目以降のアクセスであって、かつT（100）がその間に更新していた場合には、誤ったT（100）のIPアドレスを得る為に、T（100）以外のホストにアクセスしようとしてしまうことをいう。

このキャッシュの生存時間の問題を解決する為に、S202では、S－1（000）からD（000）に対して名前問合せ（正引き）をしている。

図25に名前問合せの出力の例を示す。下線部がD（000）に対して最後に更新されたT（100）のIPアドレスである。この出力結果に文字列処理を施し、下線部のみを抽出し、T（100）のIPアドレスを得る（S204）とこれを記憶装置に一時的に保存する。より正確には、次のステップでする到達性確認の為に、あて先であるT（100）を示す住所に代入する。

図26に名前問合せでエラーになった場合の出力の例を示す。DNSサーバが正しくない場合かDNSサーバがダウンしている場合の例である。

図27に名前問合せのエラーになった場合の出力の例を示す。T(100)が見つからなかった場合(T(100)を示す情報がDNSレコード中に存在しない場合)の例である。

キャッシュ問題の実例から、T(100)のIPアドレスの確認は、S-1(2000)のリゾルバがD(1000)を向いている場合や、D(1000)のTTL(キャッシュの生存時間)の設定が極めて短い場合等は、省略することができる。

S204では、必要に応じて図24のようなエラーチェックをするとよい。D(1000)で障害が発生している場合には、S204で受取る返事が不整なものになる。S204で受取る返事の中にT(100)を示すデータが含まれない場合をS402において検出した場合は、エラーとして扱う。また、Dからの返事がない場合も、同様にS402においてエラーとして扱う。この際、冗長化されたD(1000)の範囲で別のD(1000)に切り替えてみたり(S408乃至S410)、それでもだめな時は処理を中止するようにするとよい。ここで中止された場合には、T(100)の状態が仮に正常であったとしても、T(100)への到達性はないと判断されることになる。また、D(1000)の信頼性がじゅうぶんある場合には、このエラーチェックは省略することができる。この項ではD(1000)の冗長化範囲内での巡回について説明した。

サイン・アンド・カウンターサイン

S206ではS204で求められたT(100)のIPアドレスに対して、あらかじめ合意された方式での通信すなわちサインをおこなっている。なお、アドレス確認が省略できるときには、あえてIPアドレスに変形する必要はない(この場合でも、DNSを正引きした際に得られるIPアドレスで問合せをおこなう)。S208では、S206の返事が返ってきた場合には返ってきた返事を一時的に記憶し、S206の返事が返ってこなかった場合には、S206の終了コードを一時的に記憶する等して、S216のエラー処理へ進む。

図28に、SNMPのGetRequest命令でT(100)のホスト名を引いた場合の出力例を示す。

図29は、S206の通信に失敗した場合として、キャッシュの生存時間の影響等でホスト名が間違っていた場合すなわち相手先ホストがSNMPを受付けるよう設定されていなかった場合、あるいは相手先ホストが存在しなかった場合の例を示す。

図30は、S206の通信に失敗した場合として、相手先はSNMPを受付けたがコミュニティ名が間違っていた場合の例を示す。

S208では、前記図29および図30の場合等のように、T(100)がS-1(2000)からのSNMPのGetRequest命令を受付けなかった場合のエラー処理をしている。図29や図30等のSNMPのGetRe

quest命令でエラーとなった場合には、S206の返事はエラー出力のみに返され、標準出力には何も返ってこない。このような場合には、終了コード（エラーを示すもの）をフラグとして代入する等の対応を取ればよい。

図31に、SNMPのオブジェクトIDの指定間違いの場合を示す。この場合は該当するオブジェクトIDの値が正常に返され、SNMPのGetRequest命令におけるエラーにはならない為に、S212で判定されるべきである。例ではsysLocationを用いている。

その外、S206の通信が正常であってかつ合意された返事と違う内容の返事が返された場合すなわち答えられるべき返事でなかった場合には、S212で判断される。

S210では、この通信の返事に対して、文字列処理をして、T（100）のホスト名（FQDN）を抽出する。

S212では、この返事をS－1（2000）に設定された、T（100）からの返事であるべき、あらかじめ合意された方式での通信に対する答えられるべき返事との比較をおこない、判定する。

あらかじめ合意された方式での通信に対する、S－1（2000）に記憶されたT（100）からの答えられるべき返事と、S－1（2000）からの問合せ（合意された方式での通信）に対して実際にT（100）が答えてきた返事とが一致した場合S214では、T（100）は正常に動作し正しい到達性を有するホストである。

出力

ここでS214およびS216の結果表示の出力手段であるが、標準出力、キーボードとディスプレイ装置からなる通常のコンソールあるいは端末装置に出力してもよいし、記憶装置に保存されるログファイルとして書出すか、あるいはSyslogやX、SNMPTRAP等のTCP／IP上の通信路を経由して別のホストに出力してもよい。また、SMTPサーバプログラムへの入力として接続することによってメール送信でき、後述する保守に連係させる際に都合がよい場合もある。これらは複数を組合せて出力してもよいし、もちろん紙媒体へ印刷出力してもよい。本発明を実施する場合には前記の出力方法からその環境に最適な方法で出力するか、あるいは後続する処理に進むようにするとよい。

出力は到達性確認の結果の真偽によって分類される。

真の場合が、S214である。

この場合の出力は、障害検知を目的とする場合は、何も出力しなくてもよい。

その他の目的の為には、単にT（100）に対して正しく到達している旨を表示すればよい。表示する場合は、前記出力方法から最適な方法ですればよい。

偽の場合が、S216である。

一致しない場合S216は、T (100)はインターネットに接続されていないか何らかの問題でD (000)に対する更新が出来ない状態にある。

S216では、到達不能理由をS 208で返事がなかった場合か、S212で一致しなかった場合かを分けて表示することも可能である。この場合はメッセージ内容に到達不能理由を示して、ログファイル等に書出すようにした方がよい。

ところで、T (100)がD (000)に更新要求したタイミングと偶然重なった為にT (100)で障害が発生しているように見えてしまう場合等は2回目の監視タイミングまで待てば、自然と正常状態に収束するはずである。このような場合を考慮するならば、この時点では障害として検出しない方がよい場合がある。

S－1 (000)では監視プログラムをタイマ実行しているため、図示しないS 216の次のステップで、エラーフラグをたてることにより、S２１６のステップを通るのが、1回目なのか、2回目以降なのかを別々に検出することができる。なお、正常復帰時には図示しないS２１4の次のステップで、エラーフラグを消去した方がよい。

タイマ実行による2回目のS 216では、タイミングの問題ではなく、T (100)が見失われていることが明らかなので、単にログファイルに書出すだけではなく、アラートをあげるなりポケベルを鳴らすなりメールにて通知する等の方法で、保守亦は復旧をうながすようにするとよい。この場合は、到達できないT (100)そのものに通知することはできないので、T (100)の管理者宛に連絡のつく方法で通知するべきである。ただしこの場合にも、以降の表現においてT (100)に対して通知するという

この時、必要であって保守亦は復旧段階へ移行する場合にあって、T (100)が何らかの理由でインターネットから切断された状態にある時等の、T (100)が発見できないか亦は、T (200)のみが発見された場合においては、T (100)は、S－1 (000)から見失われているため、一般にアクセスするには、T (100)の設置場所に行かなくてはならない。しかし、これでは障害からの迅速な復旧をはかることができない。図１４におけるS－1 (000)からT (100)に向かう線のように、例えば、T (100)あるいはT (100)に接続されたLAN上にシリアルコンソールを用意しておき、電話回線等が考えられるが第二の保守経路を経由してT (100)の復旧をはかる等をするとよい。

実施例２

実施例1と同様の環境であって、かつ同様にＳＮＭＰをあらかじめ合意された通信の方式に用いるものであって、sysNameの替わりに、ｓｙｓNameと比較して使うことの出来る文字列の制限が少ないｓ

ysLocationを用いる事もできる。sysLocationを用いる場合には、一般に「答えるべき返事」の値にBの置換え後の文字列を用いる場合である。ただし、Bそのものを用いることもできる。この場合は、sysLocationにBそのものを設定すればよい。

なお、設定に必要な項目は表02を参照されたい。

実施例1および実施例2は、ともに合意された通信の方法にSNMPを用いるものであるので、その注意点を以下に挙げる。

SNMPは通信可能な状態であれば、T(100)のシステムの状態をほぼ何でも知りうる。また、設定変更も可能である。

本発明はSNMPの強力な管理機能を利用することが目的ではなく、見失われがちな動的IPアドレス割当てを受けた本来なら特定できないホストが、本当に意図している相手として正しいかどうかを確認しようとするものである。ここで、後続する従来の管理に接続しようとするならば、後続する管理の方法はSNMPである可能性が高い。この場合、SNMPはT(100)において既に利用可能な状態となっているはずのものなので、この環境をそのまま利用するものとして、SNMPを真偽の判定に用いてみた(後続する管理が不要な場合やSNMP以外の方法で到達性確認をおこなう場合については後述する)。

SNMPを合意された通信の方式(すなわちサイン)に用いる上で、セキュリティ上、以下の点に注意した方がよい。本発明では実験環境としてコミュニティ名は初期値であるPUBLICを用いたが、初期値のままでは侵入者を含め誰でもアクセスできてしまうため、本番環境ではPUBLICやPRIVATE等の初期値を決して用いてはいけない。また、T(100)側においてS-1(2000)のIPアドレスがわかっている場合には、S-1(2000)のIPアドレス以外からのアクセスを受付けない等のアクセス制御もあわせておこなうべきである。

実施例3

実施例1および2はT(100)が直接ダイヤルアップしていた。実施例3では、T(100)が直接ダイヤルアップするのではなく、間に網接続機器が介されており、この網接続機器がダイヤルアップする場合である。

ISDNルータ等と呼ばれるダイヤルアップルータ、あるいはブロードバンドルータ等と呼ばれるPPPoE、PPPoA、DHCP等によってIPアドレスを取得できIPマスカレード等の動的なネットワーク・アドレス変換(以下、「NAT」とする。NAPTを含むものとする)を用いてLAN上の複数のパソコンにグローバルサービスを受けさせるような網接続機器(以下、「NATBOX」とする)がダイヤルアップし、

T 4100)はカスタマのＬＡＮにのみ接している場合 図３７の接続形態４乃至接続形態６のいずれかを参照)には、網接続機器に静的ＮＡＴあるいはポートフォワーディング等の設定をすることによって、T 4100)が直接ダイヤルアップしていなくても 直接インターネットに接していなくても)実施例 1や実施例 2と同様に S－ 1 2000)から真偽の判定ができる。

この場合の条件はダイヤルアップする機能がT 4100)でなく網接続機器であること、静的ＮＡＴあるいはポートフォワーディング等の設定が網接続機器になされていること等をのぞけば、T 4100)にＳＮＭＰエージェントを実装されておりかつ設定されていることを含め、実施例 1および 2と同様である。

実施例４

実施例 3と同様に計算機が直接にダイヤルアップするのではなく網接続機器がダイヤルアップする場合において、ダイヤルアップルータ等の網接続機器がＳＮＭＰを実装していれば、これをT 4100)として利用することが出来る。

伝統的なＵＮＩＸの考え方では、 IPアドレスを割当て可能な装置はすべてホストと呼ばれる。本発明では、この考え方を援用してルータやＮＡＴＢＯＸであろうとも、 IPアドレスが割当てられていれば すなわち通信ノードでありさえすれば)、ホストと呼ぶこととする。すなわち、実施例 4ではダイヤルアップするルータがT 4100)たるホストである。T 4100)はＳＮＭＰを実装していることからダイヤルアップルータ等の網接続機器である 図３７の接続形態 2参照)が、この際に、前記ルータに IPマスカレード等の動的ＮＡＴの機能があれば、前記ルータにＤＮＳへの動的更新する機能がない場合でも、 LAN上のパソコンにＤＮＳ更新させることもできる 図 37の接続形態３を参照)。

この場合においては、ダイヤルアップルータにD 1000)に登録され動的更新されるホスト名と同じ名前を設定すれば実施例 1と同様にＳ－１ 2000)からT 4100)の真偽を判定することができる。しかし、実施例2のようにsysLocat ionを用いてより柔軟な任意の文字列を、T 4100)が返すべき返事として合意した方がスマートな構成となる。

実施例５

実施例 5は、あらかじめ合意された通信の方式に、ＤＯＭＡＩＮ DNS)を用いるものである。

T 4100)は計算機であり、ＢＩＮＤを実装しており、バージョン情報が設定 明示的に変更) されているものとする。ここでは、あらかじめ合意された通信の方式にＤＯＭＡＩＮ DNS)を用い、双方で合意された返事にこのバージョン情報を用いるものとする。

T 4100)は、直接ダイヤルアップ接続しているか、あるいは網接続機器経由で静的ＮＡＴあるいは

ポートフォワーディングの設定がされているもの とする。

S－1 (2000)では、監視プログラムをタイマ実行している。

その他の条件や設定内容は実施例 1と同様とする。

準備段階として、以下の件が合意され設定されているものとする。

T (100)に設定される、あらかじめ合意された方式での通信に対する答えるべき返事はT (100)で動作するBIN Dが返す任意の文字列に変更されたバージョン情報とする。

グローバルなインターネット向けの名前サービスを提供していない場合でも、局域的なＬＡＮ環境の為にT (100)はＤＮＳサービスを提供することができる。

図32に、T (100)において設定する、ＢＩＮＤにおけるバージョン情報の設定の仕方を示す。

ＢＩＮＤの標準的な動作として、このバージョン情報は明示的に設定されていないと、図３５のように通常はプログラムそのもののバージョンを返す。もともとは網を経由した攻撃者に対して、プログラムのバージョン情報がわかると攻撃する時の方法も明らかになるので、攻撃者の手間を増やす為に、バージョン情報をわざと変更していたものである。しかし任意に設定できることから、Bの置換え後の文字列を答えるべき返事として、ここでは例示する。

ふたたび図２３を参照されたい。

S202およびS204はアドレス確認である。実施例1と同様である。

S206では上で求められたT (100)の IPアドレスに対して、あらかじめ合意された方式での通信をおこなっている。

S208では、返事が返ってきた場合には返ってきた返事を一時的に記憶し、返事が返ってこなかった場合には、Ｓ206の終了コードを一時的に記憶する。

図33に、ｄigでＢＩＮＤにおけるバージョン情報を引いた場合の出力例を示す。下線部がＳ－１(2000)に設定された、T (100)からの返事であるべき、あらかじめ合意された方式での通信に対する答えられるべき返事にあたる部分である (図32下線部)。

ここには任意の文字列を用いることができるが、答えるべき返事の類型に従う

図34に、T (100)がかつて割当てられていた IPアドレスを現在割当てられているホストが存在しない場合および、T (100)がかつて割当てられていた IPアドレスを割当てられているT’ (200)が存在する場合であって、そのT’ (200)でＢＩＮＤが動作していなかった場合を示す。

エラー出力に出力されるエラーのみ四角で囲んであり、その他は標準出力に出力されるエラーである。

図35に、T (100)がかつて割当てられていた IPアドレスを割当てられているT’ (200)が存在する

場合であって、そのT'(200)でＢＩＮＤが動作していた場合を示す。この場合はdigコマンドの出力としてはエラーにならない為に、Ｓ２１２で判定されるべきである。

S210では、この通信の返事に対して、文字列処理をして、T (100)で動作するBINDのバージョン情報を抽出する。

S212では、この返事を、S－1 (000)に記憶された答えられるべき返事との比較をおこない、判定する。

カウンターサインによってT (100)からキャリーされた答えるべき返事とS－1 (000)に記憶された答えられるべき返事とが一致した場合Ｓ２１４では、T (100)は正しい到達性を有するホストである。Ｓ２１４では、実施例1と同様にログファイル等に書出すなり後続する通常の監視へ進むなりした方がよい。

一致しない場合Ｓ２１６でも、実施例1と同じようにすればよい。

実施例６

実施例6は、あらかじめ合意された通信の方式に、ＳＭＴＰを用いるものである。

T (100)は計算機であり、SMTPサーバを実装しているものとする。ここでは、あらかじめ合意された通信の方式にＳＭＴＰを用い、双方で合意された返事にT (100)のホスト名（FQDN）を用いるものとする。

T (100)は、直接ダイヤルアップ接続しているか、あるいは網接続機器経由で静的ＮＡＴあるいはポートフォワーディングの設定がされているものとする。

S－1 (000)では、監視プログラムをタイマ実行している。

その他の条件や設定内容は実施例1と同様とする。

T (100)に設定される、あらかじめ合意された方式での通信に対する答えるべき返事はT (100)に設定されたホスト名そのものとする。

ＳＭＴＰサーバに接続した時には多くの場合、図３６のようなメッセージを出力する（例はSMTPサーバとして最も普及しているＳＥＮＤＭＡＩＬの場合であるが、ＳＥＮＤＭＡＩＬに次いで普及しているＱＭＡＩＬの場合でも、メッセージ中にホスト名が含まれるか含めることができる）。

このメッセージには、ホスト名がＦＱＤＮで表示（図36下線部参照）されているので、これをT (100)が到達可能であるかどうかを判定する識別子すなわち答えるべき返事に用いることができる。

実施例７

実施例7は、あらかじめ合意された通信の方式に、ＨＴＴＰを用いるものである。

Ｔ(100)は計算機であり、ウェブサーバを実装しているものとする。ここでは、あらかじめ合意された通信の方式にＨＴＴＰを用いる。すなわち、Ｔ(100)で待受けするサービスがウェブサーバであることから、双方で合意された返事には、どのような文字列でも用いることができる。

Ｔ(100)は、直接ダイヤルアップ接続しているか、あるいは網接続機器経由で静的ＮＡＴあるいはポートフォワーディングの設定がされているものとする。

Ｓ－1(000)では、監視プログラムをタイマ実行している。

その他の条件や設定内容は実施例1および2と同様とする。

Ｔ(100)に設定される、あらかじめ合意された方式での通信に対する答えるべき返事はＴ(100)で動作するＨＴＴＰサーバが返す文字列中に埋め込まれた任意の文字列とする。

計算機系の技術者以外の人にとっても馴染み深いものである為に、おそらくウェブサーバは、Ｔ(100)もしくはカスタマの網におけるＴＣＰ／ＩＰサービスを提供するサーバにおいて、最も提供したいサービスのひとつだろう。ＨＴＴＰでは、どのような文字列でも転送することができることから、これを合意された通信の返事として利用可能である。多くのウェブサーバはファイル名の指定がない場合は、index.htmlという名前のファイルが開かれる(ウェブサーバからクライアントへ転送される)。ここに返事となるべき文字列を記述しておくだけでよい。例えばトップページのindex.html中、本文の3ワード目の文字列を合意しておく等である。しかし、これでは更新の際に誤って本文の３ワード目の文字列を変更してしまったりすることがあるので、別のファイル名を合意しかつそのファイル中の特定の文字列を返事として合意しておいた方がよい。また、ＨＴＭＬ文の<ＭＥＴＡ>文中に埋め込むこともできるし、<ＴＩＴＬＥ>を合意した返事として用いることもできる。要するに、ＨＴＴＰを用いる場合には、合意された通信の方式と意図された返事の境界があいまいになる。例えばＵＲＬ中に特定のディレクトリ名とファイル名を含む場合、これは通信の方式と考えるべきであろう。では、ここで転送されたＨＴＭＬ文中の本文の3ワード目は、返事とみなすべきだろうか？　これもやはり通信の方式として合意すべきだが、実施例1や実施例2、あるいは実施例5のようなプロトコルによる制約がない分、より具体的な合意が必要であることに注意した方がよい。

また、ＨＴＴＰＳを合意された通信に用いる場合であって、Ｔ(100)にＳＳＬサーバ証明書が組み込まれている場合には、ＳＳＬサーバ証明書のシリアルナンバやフィンガープリントか、あるいは単にオーガニゼーション名やカンパニー名、サーバ名等のいずれかを利用することもできる。

実施例1や実施例2の場合は、Ｔ(100)の確認をするＳ－1(000)以外からのアクセスを制限する方向であったが、実施例1や実施例2と違い、通信の方式にＨＴＴＰを用いる場合は、むしろ公開サ

ーバとして、より多くの人から確認できるようにしたい場合に有効であろう。

ところで、ＨＴＴＰは通常ＴＣＰポートの80番で待受けするが、しばしば別のポート番号に意図的に変更して待受けされることがある。このような場合でも、変更されたＴＣＰポート番号がＳ－１（2000）とＴ（100）の間で合意されていれば、Ｔ（100）が正しい到達性のホストであるか否かを確認する為に用いることができる。

また、静的ＮＡＴでもポートフォワーディングでもないが実施例３との複合型として、ＮＡＴＢＯＸは、例えば88番ポートでＮＡＴＢＯＸ自体の設定変更のためのウェブアクセスを受付け、80番ポートでリバースプロクシが動作しているような場合には、リバースプロクシによる転送先ウェブサーバにおいて、実施例７のあらかじめ合意された通信を実装可能である。

以上実施例１乃至実施例７は、答えるべき返事をどのように返すかについて説明してきた。ここでは理解されやすいように、既存のＤａｅｍｏｎを利用して説明してきた。これが流用の例である。この際には「⑤の過程を担う者」で説明したように、Ｔ（100）を実装すべきである。

実施例８

実施例１乃至実施例７におけるＴ（100）側の接続形態について、説明する。

実施例８では、Ｔ（100）がダイヤルアップルータあるいはＮＡＴＢＯＸ経由で接続している場合とＴ（100）が直接ダイヤルアップをしている場合とを問わず、Ｔ（100）の記憶装置に任意の情報を答えるべき返事として保存し、あらかじめ合意された任意の方式での通信に対して前記保存された情報を記憶装置より読み出し、少なくとも前記情報を含めた返事を返信することさえ出来れば、通信の方式を問わずにＴ（100）が正しい到達性のホストであるか否かを確認する為に用いることができる。この例は実施例７の通常でないＴＣＰポートで待受けするウェブサーバの例を既に挙げた。あるいはＦＴＰサーバへクライアントが接続する際に表示されるウェルカムメッセージもあらかじめ合意された通信の方式として用いることができる。その外、Ｓ－１（2000）とＴ（100）の間で合意されていれば、独自プロトコル等の一般的でない（ウェルノウンでない）通信の方式でも同様に合意された通信の方式として用いることができる。

Ｔ（100）は、機能的に以下に分割され得る。ａのダイヤルアップするホスト、ｂのＤ（1000）へ動的更新をするホスト、ｃのＴ（100）の機能を有するホストである。これらの機能は、各機能毎に異なるホストに分散されていてもよいし、各機能が１のホストに集約されていてもよい。これらの関係は、網の接続形態によって影響される。

T (100)のカスタマ網における接続形態を図37にまとめる。

モデム上部の雷型の線は電気通信回線を意味し、その上部にある楕円は網の雲を意味する。最上部の小さく描かれた四角がS－1 (000)である。

モデムとは、通常変復調装置を指すが、ここではケーブルモデムやＡＤＳＬモデム (やTA)等を あるいはデジタル回線終端装置 (←Digital Service Unit)や光終端装置 (←Optical Network Unit)等があるときは、説明の便宜上これをも)含み、ルーティング機能を提供しない、通信路上の物理的な境界を構成する装置を指すこととする。図３７ではモデムを独立した装置として描いたが、網接続機器や計算機に組込まれている場合がある。モデムに類する機能が、網接続機器や計算機に組込まれている場合には、網接続機器や計算機としてあつかうこととする。よって本説明では、モデムは通信の機能上必要なものであっても、ＴＣＰ／IP的な網境界を構成しないことから、モデム単独については考慮しないものとする。

図37で、モデムのすぐ下に描かれているものは、必ずダイヤルアップする機能を有するものである。これに属するものは、網接続機器と計算機がある。

網接続機器とは、ルーティング機能あるいはプロトコル変換機能を提供し、ＴＣＰ／ IP的な網境界を構成する装置を指すこととする。図３７では、 ルータ等」と表記している。

計算機とは、利用者によってプログラム可能なものを計算機と呼ぶこととし、仮に計算機が網接続機器と同様の機能を有している場合であったとしても、この点において網接続機器と区別されることとする。利用者端末等もこれに含まれる。

以下各接続形態に応じて、T (100)がどの装置であるかを中心に説明する。

実施例 1の典型を接続形態 1とする。これは、計算機が直接ダイヤルアップする場合である。実施例 2も同じである。この形態では、bのD (000)を更新するホスト、αのT (100)の機能を有するホストがaのダイヤルアップするホストと同一の場合である。この場合において、aのダイヤルアップするホストすなわち計算機が網境界を構成する。このことから、例えばＮＡＴを実装している場合やＶＰＮトンネリングしている場合のように網接続機器の機能を有しているか、アプリケーションゲートウェイを構成していれば、破線部分の計算機に対して、網接続を提供することも可能である。

実施例 4は、網接続機器を介して計算機が接続される場合であって、網接続機器がαのT (100)の機能を有するホストである場合である。典型例が接続形態 2である。また、接続形態2に対して、網接続機器がD (000)を更新できない場合に、bのD (000)を更新するホストを計算機とした場合が、接続形態 3である。

実施例3および実施例5乃至実施例7では、aのダイヤルアップするホスト、bのD（1000）を更新するホスト、cのT（100）の機能を有するホスト等が機能的に分割され、この機能が計算機および網接続機器に分散されている場合である。この場合の典型が接続形態6である。ここで、例えば接続形態4の場合は、網接続機器がD（1000）を更新できる場合であって、かつT（100）たりえない（すなわちbの機能があって、cの機能がない）場合にこのような構成をとることができる。なお、接続形態4乃至接続形態6において、aのダイヤルアップするホストはルータ等とされているが、接続形態1の応用としてこれは計算機によっても代替し得る。ここで、網接続機器がダイヤルアップすることを明示している実施例3および実施例4を除けば、一般に計算機は網接続機器と比してソフトウェアを追加することによってcのT（100）の機能を有するホストとしてもbのD（1000）を更新するホストとしても用いることができることから、接続形態1はどの実施例にも用いることができる。すなわち実施例3および実施例4（網接続機器がダイヤルアップすることが明記されている場合）を除き、aの位置にあるルータ等は計算機であってもよい。この場合、aのダイヤルアップするホストには、少なくともcのT（100）の機能を有するホストに対して静的ＮＡＴあるいはポートフォワーディング等が設定されているものとする。図37ではモデムのすぐ下にaのダイヤルアップするホストがあるが、この下には計算機だけではなく、網接続機器があってもよい。これはカスタマ網を構成するＬＡＮが多段のＬＡＮを構成していてもよいことを示す。

実施例5乃至実施例7は、すべての接続形態で用いることができる。ただし、実施例5乃至実施例7を接続形態2や接続形態3に適用する場合には、網接続機器がサインに対し、答えるべき返事をキャリーするカウンターサインを返し得るように構成できる必要がある。

aのダイヤルアップするホスト、bのD（1000）へ動的更新をするホスト、cのT（100）の機能を有するホストは、同一のＬＡＮ上（あるいは同一の場所）に設置されるものとするすると、広域の網から見れば、このＬＡＮは網端側にあることになる。ここで広域の網をインターネットとした場合（正確にはＮＡＴを必要とする場合）、広域の網を経由した通信では、a、b、cのそれぞれを識別することはできない。よって、このＬＡＮは外部に対して単一の通信ノードのように振舞う、計算機および網接続機器の集合である（インターネット・サービス・プロバイダーへの端末型ダイヤルアップのようにＬＡＮを構成しておらず、端末一台のみの場合にあっても同じである）。これを本発明では、カスタマ網もしくはエンドサイトと呼ぶこととする。エンドサイトは特に広域の網から見た場合のエッジ側を指すものとして扱うが、着目点が違うだけでカスタマ網と同じ物を指している。図37のモデム以下の点線で囲まれた部分である。接続形態1から接続形態6は、カスタマ網の内訳であり、S－1（2000）から見れば、カスタ

マ網が接続形態1から接続形態6のいずれの類型に属していようと、a、b、cのそれぞれを識別することはできないという点で共通している。そのため、S－1（2000）ではカスタマ網の構成やT（4100）がカスタマ網のＬＡＮ上でどこに、位置しているかについて考慮する必要がない。

なお、カスタマ網はプライベートIPアドレスが使用されている状態を仮定している。このため、インターネットからは、カスタマ網に対して、直接ルーティングされることはない。aのダイヤルアップするホストは、インターネットとカスタマ網の接点を構成する。ルーティングはaのダイヤルアップするホストで止まるから、インターネットからb、cには直接到達できない。

上記は、広域の網をインターネットとした場合であった。

ところが、広域の網としては、インターネット以外にも、第一種電気通信事業者や第二種電気通信事業者が提供するかあるいは自営網によるインターネットに接続されない、ＴＣＰ／IPによる網が考えられる。この場合には、ＮＡＴを前提とするのでなく、ルーティングによって別の網にあるD（1000）やS－1（2000）からT（4100）へのアクセスが、直接にT（4100）に到達できる場合がある。

実施例1乃至実施例7では、説明上インターネットと表現してきた。しかし、グローバルなインターネットでのみ本発明は実施可能なものではなく、実際はＴＣＰ／IPを用いた通信でありさえすればよい。

カスタマ網と外部網の関係を表03に示す。

表03）

			WAN	DNS（D）	ルーティングによる到達性	ネットワーク境界における 接続するネットワークの数	ネットワーク境界における 管理対象機器のI／F
インターネット（= the Internet）の場合		①	あり	公共	WAN側まで	1（WANのみ）	選択の余地なし
		②			WAN側まで	2以上（LANとWAN）	WAN側のI／F
インターネットに接続されない広域の網の場合	電気通信事業者が提供する役務の場合	③	あり	私設	WAN側まで	1（WANのみ）	選択の余地なし
		④			WAN側まで	2以上（LANとWAN）	WAN側のI／F
	自営網の場合	⑤			あり	1（WANのみ）	選択の余地なし
		⑥			あり	2以上（LANとWAN）	WAN側のI／F
LANのみの場合		⑦	なし	私設	不要	1（LANが一段）	選択の余地なし
		⑧			あり	2以上（LANが多段）	上流のI／F

①は、インターネット・サービス・プロバイダーへの端末型ダイヤルアップのようにＬＡＮを構成しておらず、端末一台のみの場合を指す。この場合はＬＡＮを構成していないが、インターネットに接している為に、やはり網に接続されている（スタンドアロンではない）ものとみなす。ＬＡＮを構成してい

ないことから、カスタマ網は存在しないのではとの議論がありうるが、ループバックのみのカスタマ網が存在し、ＷＡＮ接続されているものと考えればよい。③および⑤は、①に準ずるものとする。

②は、代表的なインターネット接続の場合である。これまでの説明は、このパターンを想定して、説明してきた。以下、このパターンとの相違点がどのように影響するかについて、説明する。

④は、第一種電気通信事業者や第二種電気通信事業者が提供するインターネットに接続されない、ＴＣＰ／ＩＰによる網をＷＡＮとする場合である。パソコン通信やフレッツ（登録商標）オフィス等がこれに該当する。②の場合と同様に扱って問題ない。Ｄ（1000）が私設のものであることは、従来からあるプライベート網に使用するドメイン名の命名規則において制限があるのみで、本発明には影響しない。

⑥は、自営網による場合である。自営網は一般に組織内の利用の為に、専用線（および類似の役務。例としてＡＴＭメガリンクやＩＰ－ＶＰＮ等を挙げておく）等によって構成され、ルーティングされているものをいう。④の場合は、ＩＰ－ＶＰＮ等の契約がなければ通常はカスタマ網（の内側。網端までは当然に到達するので）へのルーティングは提供されない。しかし、第一種電気通信事業者や第二種電気通信事業者が提供する役務であって、ルーティングがされる場合は、⑥に含めて考えた方が筋道がよい。網境界を越えて、外部網がルーティングによって直接にカスタマ網上のホストにアクセスできる場合である。すなわち、この場合は、Ｔ（100）がモデムのすぐ下に位置しない場合であっても、ａのダイヤルアップするホストは上流の網からＩＰアドレスを動的に割当てられるのではなく、カスタマ網上のＤＨＣＰサーバ（ＤＨＣＰリレーされている場合を含む）からＩＰアドレスを動的に割当てられ、かつＴ（100）であるという点で、図３７の接続形態１乃至接続形態３に相当することになる。ところで、古くから自営網を運用している会社や大学の中には、IPアドレス体系がグローバル・アドレスになっているところがある。このような自営網は、インターネットそのものの構成要素であるものと考えてさしつかえない。

⑧は、ＬＡＮのみで構成された網にあって、ＬＡＮが多段となっている場合である。例を挙げると、１の事業所であって、フロア毎に別の部に分かれている場合に、各フロアが事業所内バックボーン（網を経由して相互に接続されている場合等である。ＷＡＮが存在しておらず、インターネットに接続しない場合やインターネットに接続しない広域の網に接続しない場合か、仮にインターネットに接続していたとしてもこの接続を無視できる（セキュリティポリシが強力な組織等にあってインターネット等へ接続する際に障壁が大きい）場合であるという特徴を除けば、自営網の場合と酷似する。ここで、ＬＡＮが多段になっているとは、単にハブ等によって多段となっているだけではなく、論理セグメントが分かれており、ルーティングされている状態を指す。この場合、Ｓ－１（2000）の接するＬＡＮがＴ（100）

の接するＬＡＮとは別のＬＡＮであれば、Ｔ（100）の接するＬＡＮをカスタマ網と考え、④⑥と同じと考えればよい。

以上は、物理セグメントと論理セグメントがともに分かれている場合であったが、例外として、物理セグメントが１で論理セグメントのみ２以上に分かれている場合、例えば１のインターフェースに異なる網に属する２以上のＩＰアドレスを割当て、これを中継するよう構成されたゲートウェイ装置等がある場合には、単一の（＝一段の）ＬＡＮの場合と同様となる。

⑦は、単一のＬＡＮの場合である。本発明は実施可能だが、ＬＡＮが一段のみの場合すなわち外部網がまったく存在しない場合には、ＴＣＰ／ＩＰ的な中継を要せず、各ホストがすべて直接かつローカルに通信できるので、動的ＩＰアドレス割当てのホストであっても、わざわざ私設のＤ（1000）を参照することなく、ＴＣＰ／ＩＰ以外のプロトコルによって、到達性確認をした方が現実的であろう。

当然のことであるが、Ｔ（100）がスタンドアロンの場合を、本発明では考慮していない。通信する相手が存在しないからである。

なお、②④⑥の場合は⑧と共存する。

以上によって、（⑦の場合に意味があるかどうかは別論だが）①乃至⑧のすべてのパターンで本発明を実施可能である。

ここで図３８に、主に多段のＬＡＮの場合に問題になり得る点について説明する。図３８は、カスタマ網におけるＬＡＮの内訳でもあるが、自営網の場合およびインターネットに接続されない電気通信事業者が提供する役務の場合も同様であるものとし、この場合にあってはカスタマ網はＴ（100）が直接接続されている部分を指すものと考えられる。網１および網２は、それぞれＬＡＮの場合とＷＡＮの場合がある。

図３８には、パターン１乃至パターン３までを挙げた。パターン２およびパターン３は、表０３における④⑥と類似のパターンであって問題がない。ここで問題となり得る場合は、パターン１の場合であって、網１がＬＡＮの場合である。表０３における⑦に挙げた単一のＬＡＮの場合と同様に、Ｔ（100）とＳ－１（2000）とが同一のＬＡＮ上にあるため、ＴＣＰ／ＩＰ以外のプロトコルによって、到達性確認をした方が現実的と考えることができる。しかし、この場合であっても、別の網上にＴ（100）が存在し、かつここでいうＳ－１（2000）が前記Ｔ（100）をも管理するものとすれば、本発明を実施する意義はじゅうぶんにあると考える。なぜならば、別の網上のＴ（100）を管理する際には、本発明の実施が必要なものであって、Ｓ－１（2000）が集中管理する為には、管理の方法を統一した方がよいからである。なお、表０３の⑧においてパターン２のように装置が配置されている場合は、Ｔ（100）から見てＳ－１

2000)やD 1000)が外部の網に属しているという点で、表03の②④⑥の場合に相当する。

なお、ＴＣＰ／IP以外のプロトコルはルーティングされないものとする。

P 4000)はT 4100)を含む網であると考えられるので、今度はP 4000)の観点から、機能が複合した場合の特徴について説明する。なお、図38ではT 4100)を含む網1がP 4000)にあたる。P 4000)がＤＨＣＰである場合であっても、網1はＤＨＣＰサーバを含む網であるとして、以下説明する。また、網2はここでは単に網1でない網とする。

機能が複合した場合の特徴

S－1 2000) とP 4000)が一体となっている場合。図38のパターン１の場合である。

P 4000)の網に属するT 4100)に関して、後述する条件1によって、S－1 2000)は本発明によらずにT 4100)の到達性を確認出来る。しかし、T 4100) とD 1000)は異なる網に属しているため、実像と写像のの関係の正しさについて、S－1 2000)は確認することができない。すなわち、T 4100)に関してD 1000)によって獲得するホスト識別性については、本発明の到達性確認を要する。

S－1 2000) とD 1000)が一体となっている場合。図３８でいうパターン2の場合である。

アドレス確認は不要である。この他別の効果もあるが、これについては後述する実際的応用の第三のフィルタ例で説明する。

D 1000) とP 4000)が一体となっている場合。図３８のパターン3の場合である。

IPアドレスの割当て主体であるところの、T 4100)を含む網すなわちP 4000) と、D 1000) とが同一の組織に属する場合である。

先に説明したように、一般的にこの場合は問題がない。

しかし、条件1から、P 4000)がD 1000)を更新する場合は、境界線上の場合である。

条件１

P 4000)は特別な立場にある。

P 4000) とは、ここではT 4100)に対してIPアドレスを割当てるものをいう。

よって、当然にP 4000)はT 4100)のIPアドレスを把握しているものとする。

そして、当然にP 4000)はT 4100)が接続しているか接続してないかをも把握できる。

以上を条件１とする。

さらに、P－D（4500）は、逆引きの設定が可能である。（静的な識別子と動的な住所の関連付けにおける一方向性」で説明した、「DNSは正逆あるが、ダイナミックDNSは正引きのみである」と書いた前記に反する場合である。P（4000）とD（1000）が一体となっている以上、P－D（4500）はD（1000）と同一の場合であり、この場合には、管理権限の問題が発生しないためP（4000）はP－D（4500）すなわちこの場合はD（1000）を更新することができる。ただし、P－D（4500）とD（1000）が同一の場合とは、P－D（4500）がT（4100）のアナウンスする静的な識別子を公示するもの（すなわちDの機能を有するもの）である場合に限られる。

以上から、P（4000）はT（4100）の状態の変化を知ることができ、かつ、T（4100）の状態の変化をD（1000）に反映することができる。

よって、ダイナミックDNSにおけるホスト名そのものが、追従性および識別性を有する場合である。

ここでは、静的な識別子による外部の網からの参照可能性のことを、ホスト識別性という。

到達性を確認するまでもなく、もとから網におけるホスト識別性を有するホストに対しては、到達性確認のプロセスによって、はじめて真偽が分かる訳ではない。

よって、境界線上の場合である。

ただし、P（4000）とD（1000）を完全に連携させることはかなり複雑な設定を必要とする。そのため、チェックの為に本発明を用いることはよい。

また、D（1000）がDNSの場合、外部の網からのアクセスについてはキャッシュの影響を受ける。

ここまで、場合分けして説明してきたが、複雑でわかりにくいものである。これは網の接続のされ方を網羅的に説明する困難さに起因すると思われるので、以下のように、LANかWANかを問わず、ルーティングがどこで止まるかによって、大別できる。

ルーティングによって、直接T（4100）に到達できる場合にはS－1（2000）は、当然にT（4100）の1つ1つを別のホストとして識別できる。この場合においては、T（4100）は、ダイヤルアップする（動的アドレス割当てを受ける）機能と、D（1000）を更新する機能とT（4100）であることの機能を備えていなければならない。そして、この場合は、比較的単純な場合である。

ルーティングがダイヤルアップするホストで止まる場合には、ダイヤルアップするホストにおいてポートフォワーディング等によって、外部網からはT（4100）にS－1（2000）からのアクセスが到達するようにするかダイヤルアップするホストをT（4100）としなければならない。これはルーティングによって到達できる場合と比べてやや複雑であり、具体例については既に実施例として詳述した。ダイヤルアップする（動的アドレス割当てを受ける）機能と、D（1000）を更新する機能とT（4100）たる機能（す

なわちカウンターサインを返す機能亦は到達性を確認させる機能)は、独立した3のホストが担ってもまた集約された1のホストが担ってもよいが、外部からはカスタマ網の代表として、T (100)が確認されるという点で特徴がある。

実施例9

ルータ等の網接続機器であって、設定変更用のウェブインターフェースを有する場合は、ウェルノウンポート (RFC1700 ASSIGNED NUMBERS でいうところのウェルノウンポートと同じか類似するもの)に従って80番ポートで待受けする。ファイヤウォール等の一部の機器は、例えば88番ポート等の80番ポート以外のポートで設定変更のためのウェブアクセスを待受けする場合がある。最近のエンドサイト向けのこれらの製品はWAN側とLAN側に分かれてインターフェースを用意しており、多くの場合、WAN側ポートにはアクセス制御が施されている。

ここで、網接続機器において (ファイヤウォールでなくとも)、設定変更のためのウェブアクセスの待受けを88番ポート等の80番ポート以外のポートでし、アクセス制御されるものとする。この際、80番ポートで通常のウェブアクセスを待受け、これにはアクセス制御等を施さないものとする。80番ポートでリバースプロクシを動作させ、リバースプロクシによる転送先ウェブサーバにおいて、実施例8のあらかじめ合意された通信を実装可能とするのも手なのだが、ここで、装置にはホスト名が登録されるものとし (エンドサイト向け製品の内、低価格製品の多くにはホスト名の設定ができないものがある)、このホスト名は写像を公示するD (1000)において設定されるFQDNで登録されるものとし不揮発メモリ等の記憶装置に保存され、80番ポートへの通信要求を受けた際に、前記保存されたFQDNを記憶装置より読み出し、該FQDNすなわちホスト名を含めた文字列を返信するように構成する。

S (1000)がT (100)に対して通信を試みる方法として、このように実施例4のように網接続機器に対して、実施例7のようにHTTPを合意された通信の方式として用い、実施例1のように (SNMPのsysNameではなくHTTPだが) FQDNを返事として合意した方法等のように実施例を組合せた方法として用いることができる。なお、カスタマ網上の位置だが、図37の接続形態のすべての場所だけでなく、接続形態6における計算機の位置にあっても、既に説明したように機能するものであって、ここで構成した装置が網接続機器であった場合に、配下に別の網を有している場合が考えられる。また、ここで構成した装置が直接図37における aのダイヤルアップするホストである必要は必ずしもない。

このとき仮に、ここで述べた機器が図37にいうaのダイヤルアップするホストであって、網の到達性

からＮＡＴを必要とする網である場合には、80番ポートを上記のようなサイン・アンド・カウンターサインに用いてしまうと、ウェブサービスを提供する際にポートフォワーディング等が必要であるから、ウェルノウンでないポートをアナウンスしなければならなくなる。これでは、カスタマ網においてウェブサービスを提供しようとする場合の利便性をそこなうことになる。そこでウェブサービスを提供したい場合には、類似のポートでサインを待受けするようにするとよい。すなわち、ＨＴＴＰアクセスを待受けするポートにおいて、機器設定用のポート、サイン・アンド・カウンターサインを用いた網管理用のポート、一般の閲覧に供するためのウェブサービスを提供するウェルノウンなポート（ただし、ここで述べた機器が応答するのでなく、ポートフォワーディング等してもよい）のように３種類のポートで待受けするように構成することもできる。

これを実施例９とする。実施例９では通信の方式をＨＴＴＰ固定とし、返事をＦＱＤＮとすることによって、単純化した。通常、網接続機器にあっては、いわゆる計算機に比して拡張性に劣るものである。これは、例えば機能追加する際に単にプログラムを追加実装すればよいというものではなく、ファームウェアの書換え等が必要であって、利用者によっては、簡単にできない等の問題があるものである。そこで、、実施例９は、ルータやＮＡＴＢＯＸ等のように記憶装置の容量に制限がある網接続機器に対しても、あらかじめコンパクトに実装しておくことが可能である。

Ｔ（100）としては、網接続機器だけでなく、もちろん計算機であってもよいし、コンパクトに実装可能なことから、カウンターサインを返すためだけの専用の装置でもよい。この場合、専用の装置は、単にＳ－１（000）に到達性確認させるためだけの機能を有しておればよく、インターフェースももちろん１でよい。例えば、図３７の接続形態６の場合であって、ｃに位置していたとすると（図３７では計算機だが、これが上記専用の装置の場合）、ダイヤルアップするホストの外側にある網がインターネット等のルーティングによってＴ（100）に到達できない網である場合に、ダイヤルアップするホストに静的ＮＡＴやポートフォワーディング等が設定されていれば、外部網からは装置に到達可能である。この場合において、システムは単にＬＡＮ上のＩＰアドレスを割当てられていれば、外部網からは、一体となって参照される為に、ここでいう専用の装置が到達性確認することによって、Ｓ－１（000）からは、カスタマ網およびその境界ノードが正しい到達性を有することを確認することができる。つまり、ここでは、単に実施例９を実装した１のインターフェースを有する機器を準備すれば、ポートフォワーディング等の設定をダイヤルアップするホストにするだけで、到達性確認できることになる。このような装置は、単純な為に、安価に製造することができるし、完成品ではなく組込み用の基盤あるいはキットとしても提供できる。また、これをソフトウェアとして実装すれば、計算機に用いる場合でも、設定作業

を省略化することができる。この場合は、記憶装置に述べた記憶媒体読取り装置に実装される取り外し可能な記憶媒体とすればよい。

実施例10

T (100)が例えば、モバイル端末である場合に有効な方法を提案する。

ここでモバイル端末とは、例えば携帯電話そのものである場合と、いわゆるＰＣである場合を指す。ここでいうＰＣは、単に一般利用者が用いる計算機による端末を指す。

このような場合には、T (100)の機能はアプリケーションプログラムとして実装してもよい。

しかし、独立したアプリケーションプログラムとしてだけではなく、従来から存在するプログラム、例えば、ブラウザソフトの組込としてもよい。

ブラウザソフトの組込とする場合には、ブラウザソフトを答えるべき返事設定用等の制御用として用い、ブラウザソフトからコールされる別途待受け用の常駐ソフトによって、答えるべき返事を返すようにするとよい。

この際、実施例7等のように既にウェブサーバが実装されている場合にはもちろんそれを利用してもかまわないのだが、別途待受け用の常駐ソフトを用意し、別のポートでサインを待つようにしてもよい。

また、このような常駐ソフトは、停止できるように実装されてもよい。

こうすることには実は別の意図があって、実際的応用に示すS－２(300)が到達性を確認する場合の、ユーザーインターフェースとして用いることができるからである。

すなわち、ブラウザソフトは、別途コールされる到達性確認用プログラムによって、到達性確認した結果を表示するものともなる。

要するにブラウザソフトは、外部プログラムであるか内部プログラムであるかを問わずに、T (100)の機能とSの機能の両方を提供するユーザーインターフェースとして、用いることができる。

実際的応用)

到達性確認は、後続するアクションの有無によらずに、結果を表示（図23のS214亦はS216）して終了するものと考えればよい。実際的応用（←practical application）は、到達性確認の結果を用いてどのように役立てるかという用途的な分類である。

これは以下の観点から分類される。

動作モデルの観点からは、ピア・トゥ・ピア・モデルとクライアント・サーバ・モデルに。

到達性を確認する主体であるところのSは何かという観点からは、S－1（2000）、S－2（300）およびD（1000）に分類される。これを、Sの主体と表現する。

結果の表示をする相手先は何であるかという観点からは、T（100）、S－1（2000）、S－2（300）およびD（1000）に分類される。これを客体と表現する。（もちろん到達性確認の客体は常にT（100）である。ここで客体とは、結果表示を利用して利益を得る者は誰かを意味する）

何の役に立つかという観点からは、障害検知、表示、フィルタ、組A：Bの写像の消込（第三のフィルタ例）に分類される。これを用途と表現する。

以上から代表的な例をまとめると、以下の表となる。

表（4）

主体	客体	分類	用途
S－1	T	障害検知	Tの障害を検知して通知
S－1	S－1	フィルタ	Tのトラフィック監視など
S－1	S－2	表示	ping代替
S－2	S－2	表示	ping代替
S－2	S－2	フィルタ	後続する通信プログラムに接続するための前置処理
D	D	特殊例（フィルタ）	組A：Bの写像を消込

T（100）の為にする障害検知と、

S－2（300）の為にする表示は、類似の概念である。

いずれも到達性確認をping代替として用いるものである。

T（100）の為にする障害検知が、より限定的な概念であって、既に実施例1に説明したように、T

4100)の障害を検知して、T 4100)に障害対応をうながすことである。この場合のT 4100)は、通信ノードとしてのT 4100)ではなく、Tの所有者亦はTの管理者等のヒトである。

S−2 5300)の為にする表示は、より単純で広範な場合であって、T 4100)に対して正しく到達するか否かを、単に表示するものである。

フィルタとは、単に表示するだけでなく、到達性確認の結果を後続するアクションに生かそうとするものである。

障害検知とフィルタの場合は、後続するアクションが想定されているという点で、類似する。

障害検知では、後続するアクションは、ヒトによる復旧処理であった。それに対して、フィルタの場合は、後続するアクションはプログラムであって、一連の処理に組み込まれて実施されることを想定している。

ここで、T 4100)への到達不能が検知されたときに、T 4100)が障害であると考えるべきかどうかについて説明する。例えば、特許文献2では、ヘルスチェックによってT 4100)相当が到達不能である場合には、異常として検知される。本発明でいう障害検知も同様の考え方である。しかし、それ以外の場合、例えばフィルタや表示の場合等は、断続的に接続と切断を繰返すT 4100)にあっては、接続され正しい到達性を有している場合のみがT 4100) として正常であるとのスタンスは取っておらず、到達不能な場合もまた正常である。要するに、T 4100)の性質に応じる。T 4100)が常に他ホストからの被アクセス可能性を維持しなければならない場合には、アクセスできない状態は障害である。網への接続と切断を繰返す為に、必ずしもアクセスできなくてもよいT 4100)の場合には、アクセスできない状態であっても、別段障害ではない。

障害検知の場合

管理対象機器の所有者向けの通知として、メールやポケベル等が挙げられる。管理業者向けの通知として、SYSLOG、SNMPtrap 等が挙げられる。これらはヒトを対象とする通知でありながら、実際には後続するプログラムへの代入であるので、後述するフィルタに含めて考えてもよい。実施例1に詳しく説明した。

表示の場合

いわゆるping代替として（つまり単にホストへの正しい到達性があるかないかを知る為に）用いる場

合である。

公共の為にする表示とは、T (100)の到達性確認の結果が真であるとか偽であるとかを、S－2 (300)に対して表示するというものである。S－1 (200)でする場合をクライアント・サーバ・モデルでの動作とする。一般利用者の使う端末であるところのS－2 (300)でする場合がピア・トゥ・ピア・モデルである。

クライアント・サーバ・モデルの場合のS－2 (300)は、不特定多数であってよい。この場合のS－2 (300)は、網上の単なる通信ノードであって、Sの機能すなわち到達性を確認する機能を実装している必要がない。それゆえこの場合は、S－2 (300)そのもののためではなく、公共の為にする表示である。

また、この場合の到達性を確認する主体S－1 (200)は、T (100)の為に障害検知するものと同一である必要はない。例えば、主体がS－2 (300)であっても、他のS－2 (300)の為に到達性確認の結果を表示するものは、S－1 (200)であると考えればよい。ただし、S－2 (300)を主体とする場合には、単に自らの為に到達性確認する場合が一般的である。

S－2 (300)について、まとめる。

S－2 (300)は2通りある。

一般利用者であって、Sの機能を有するもの。

一般利用者であって、Sの機能を有しないもの。この場合は、クライアント・サーバ型で動作し、S－1 (200)とセットで用いる。

到達性確認の結果の利用方法として、表示の場合が最も従来のpingに近い。しかし、当然にpingの方がシンプルで応用がきく。ただしここでは、pingでは到達性を知ることのできない動的な住所を割当てられたホストに対して、到達性確認では到達性を知ることができるという点で、優位性がある。

S－2 (300)がT (100)の到達性を確認する手段として本発明を用いる場合のイメージを、図39に示す。 (a)がpingの場合、(b)が到達性確認の場合である。

従来のpingの場合は、図39 (a)のように、S－2 (300)は直接調べたい相手先のホスト名あるいはIPアドレスを指定する。

それに対して本発明では、S－2 (300)の利用者がT (100)の到達性を調べたい時には、調べたいT (100)のホスト名を指定して、S－1 (200)に到達性確認を依頼する。図39 (b)の①

すると、S－1 (200)がS－2 (300)に替わって、T (100)の到達性を確認すなわち図39 (b)の②=サイン、同③=答えるべき返事をやりとりし、

その結果をS－2（300）に通知する。図39（b）の④

これはコマンドでもよいが、S－2（300）の利用者が計算機や通信の知識がない場合にも簡易に利用することが出来るように、ウェブページを例として挙げてみる。

これはCG等によって生成される、メッセージとボタンからなる画面をイメージされればよい。

第一は、図39（b）の①のフェーズに相当し、S－2（300）がウェブページに入力する、到達性確認したいT（100）を指定する画面例である。

「到達性を確認したいホストはなんですか？」亦は「到達性確認対象ホスト名を入力してください」等のメッセージが表示されており、その下に、ホスト名の入力欄がある。そして、「実行する」亦は「確認する」等のボタンを配したウェブページを生成すればよい。なお、特許文献2の場合のように、DNSを用いない場合には、これに先立って、あるいはこの画面のオプションとして、条件を入力させるようにすればよい。この条件とは、例えば特許文献2におけるD相当の所在情報等である。

第二は、結果としての図39（b）の④を表示している画面であり、T（100）が正しい到達性の場合である。メッセージ内容はインスタントメッセンジャ風に「オンライン」や「出席」としてもよいし、亦はping風に「到達可能」としてもよい。

第三は、結果としての図39（b）の④を表示している画面であり、T（100）が到達性を有しない場合である。第二の場合と同様に、「オフライン」や「欠席」亦は「到達不能」としてもよい。第二、第三の画面では、「戻る」ボタンを配した方が親切である。

なお、この場合は、S－1（2000）がT（100）に対して到達性確認するタイミングは

S－1（2000）の内部タイマに基づいても、

S－2（300）からの到達性確認要求を受けたことをトリガとして、

到達性確認してもよい。

ところで、クライアント・サーバ・モデルの場合であって、S－2（300）がSの機能を有しない場合には、前記画面で到達可能とされても、たまたまT（100）の住所が変化した直後には、T（100）とS－2（300）間の通信において、キャッシュの影響を受けてS－2（300）からはT（100）に到達することができない場合がある。なぜならば、S－2（300）がSの機能を有しない場合にはキャッシュは無効化されておらず、当然にキャッシュの影響を受けて誤認を生じさせるからである。このとき、S－1（2000）では到達性確認をした時刻およびT（100）に対するD（1000）のキャッシュの生存時間を知ることができる。履歴情報と比較することによって、T（100）の住所が変化したことも知ることができる。

そのためS－1（2000）では、到達性確認した時刻から導き出される、S－2（6300）からの最遅アクセス可能時刻をあわせて表示するようにしてもよい。亦は、キャッシュの生存時間を示し、再度のアクセスをするよう表示してもよい。

フィルタの場合

S－1（2000）でする場合であって、従来の管理に接続するための前置処理の場合である。到達性確認の結果を、従来の管理の入力として代入することによってなる。

例：T（4100）のトラフィック計測への代入等。

方法：到達性確認済みのホストを代入させることによっての通常のSNMP管理へ接続する。

いわゆる、フィルタとして動作させる場合である。フィルタの概念は先行するプログラムの出力を、後続するプログラムの入力とする考え方である。UNIXでいうパイプの概念に相当する。例を挙げれば、ソートプログラム等がこれに類する。ソートプログラムは、何らかの出力結果を並べ直して、次の処理に接続する。

第一のフィルタ例として、本発明をセンサーとして用いる場合を挙げる。管理対象の変化を検知し、この結果を従来の管理に接続する。

後続するアクションは明らかにプログラムであって、例えばMRTGやOpenView等による通常の管理である。その他、本番の通信に先立って通信相手の到達性が確認されている必要のある場合すべてにおいて、有効である。S－2（300）たる人間が直接T（4100）にアクセスして、何らかの処理を行う場合でなく、機械によって自動化されている場合に有効である。

T（4100）が正しい到達性を有するホストであることが確認された場合には、後続する処理に接続することができる。例えばMRTGやOpenView等による従来（T（4100）が固定IPアドレスであり、到達性確認をあえて必要としない場合と同等）の監視処理をあげておく。従来の監視（＝後続する処理）の例として、ucd-snmp-4.2.1 および mrtg-2.9.17 を用いてみた。MRTGは、現在の網のトラフィックの状態および時間によって変化する情報（例えば、CPU負荷率等）をグラフィカルに表示してくれるソフトウェアツールである。MRTGはSNMPマネージャの機能を含んでいる（そのため、ここではSNMPマネージャとして扱った）が、トラフィック履歴ファイル生成用に特化している（つまりユーザーインターフェースを持たない）為に、通常は別途SNMPマネージャと組合せて用いる。従来の管理方法については、本発明の対象外なので説明しないが、接続の際に問題があったので、その解決方法については以下に説明する。ここで試験の結果、少なくともMRTGではIPアドレスが変化す

るホストに対しては、T (100)をFQDNで指定しても (IPアドレスの変化に追従できず)、通常の監視をおこなうことはできなかった。そのため、MRTGで指定するT (100)名にその時点でのT (100)のIPアドレスを代入したMRTGの設定ファイルを生成しなおす処理を追加することによって、通常の監視処理に接続した。

例えば特許文献4は、変化する下位監視対象に追随するシステムの提案であるが、下位監視対象が変化したことを検知する方法については説明されていない。

そこで本発明を特許文献4に開示された発明の、更に前段の処理 (フィルタ) として追加することによって、下位監視対象が変化したことを検知することができる。こうして検知された結果から下位監視対象のリストを作り直し、特許文献4の入力とする。この際、下位監視対象を示す静的な識別子を記述したリストから、個別に到達性確認し、正しい到達性を有するホストを対応付けたリストを作り直し、これを特許文献4の入力とするとよい。リストを作り直す処理は当然に、プログラムが行うものとする。

こうすることによって、手作業による入力なしで変動する下位監視対象に追従できるようになる。

このとき、ホスト名、現在のIPアドレスのみをプログラム間のパラメータとして受渡しするのではなく、従前のIPアドレスをも引渡すとよい。本発明の開示中、従前のIPアドレスを保存しておくことは開示していない。しかしこのような実装上の軽微な変更は本発明の本質になんら影響するものでなく、当然に本発明の開示から容易に想到されるものである。

もちろんT (100)のIPアドレスが変化した履歴情報を追跡の為に保持するような変更も、明示するまでもなく本発明の範疇に含まれる。

ところで、S－1 (2000)でするフィルタの場合、到達性確認の結果を処理として引継ぐ客体は、S－1 (2000)の場合とT (100)の所有者亦は管理者の場合とがある。ここでT (100)の所有者亦は管理者は、別途到達性のある管理用のシステムを運用しているものとする。T (100)の所有者亦は管理者を客体とする場合は、障害検知の場合を参照されたい。この際、静的な識別子と、正しい到達性を有することを確認された動的なその時点での住所を、SNMPTRAP等に含めてT (100)の所有者亦は管理者あてに通知するようにするとよい。その後は、S－1 (2000)でする場合と同じである。

ところで、本発明をフィルタとして用いる場合には、後続する処理は従来の管理に限定されるものではない。この場合が第二のフィルタ例であって、第一の例よりも更に、フィルタ然とした用法である。利用者端末であるS－2 (300)においてする場合を例示する。

例えば、「IP Messenger」というPC上で動作するフリーウェアがある。これは、通信相手のIPアドレ

スを直接指定することによって実現した、サーバ不要の（つまりピア・トゥ・ピアの）リアルタイム・メッセージ送受信ソフトウェア（註 用途が同じであっても、サーバ不要なので『P Messenger』はインスタント・メッセージング（RFC2778、RFC2779）の範疇に含まれない）である。

このようなプログラムに本発明を前置処理として実装することによって、例えば『P Messenger』は、IPアドレスといった動的な住所でなく、単にホスト名等の静的な識別子で通信相手を指定できるようになる。

更に、それだけに止まらない。

ちょうどリゾルバがありとあらゆる通信アプリケーションソフトの前置処理として動作するように、本発明もあらゆるプログラムの前置処理として動作させることができる。

なお、この場合の主体は、S－2（300）のみでなく、S－1（2000）であってもよい。

註：『P Messenger』はあて先としてホスト名指定ができるようになりました。しかし、本発明で開示した問題点は解決されていないようです）

第三のフィルタの例を挙げる。

SとD（1000）が一体となっている場合（図38パターン2参照）、というよりはD（1000）においてSの機能を実施するときには、ある特殊なことが出来るようになる。

公示された組A：Bの関連を公示しないようにする。

この方法は、マッピング公示システムD（1000）において、T（4100）に対する組A：Bの写像を公示しなくする方法である。DNSサーバの場合には、T（4100）に対するリソースレコードを消去する（以下、DNSにおけるリソースレコードの消込みは、更新の一形態として、更新に含むものとする）。D（1000）においてSの機能を実施した結果、T（4100）に対して到達性が確認出来ない場合には、その他のホストからも同様にT（4100）に到達することができないはずである。この際、誤認されたホストT'（4200）に到達するおそれがあることは、既に説明した通りである。このとき、マッピング公示システムD（1000）において、T（4100）に対する組A：Bの写像を公示しなくすることによって、誤認を生じなくさせることができる。

これは、本来的にはT（4100）がするはずのオフライン処理を、D（1000）が替わってすることである。このような提案は既にされており、特許文献1や特許文献2に開示されている。

特許文献1では、T（4100）からD（1000）へ、キープアライブ信号というものが送信され、D（1000）ではこれが受信されなくなった場合に、D（1000）で公示する組A：Bを公示しないようにしている。この場合の考え方は、ビーコンやハートビートと同様に端末から信号を送信するという考え方である。同

様の例に、特許文献5等がある。

特許文献2では、ＤＮＳを用いない独自システムではあるが、Ｄ（000）からＳへ、ヘルスチェックという処理を施している。ヘルスチェックの実体は、Ｔ（100）がＤ（000）に対して組Ａ：Ｂを設定する際に用いるパスワードを、盗聴対策の為にチャレンジ・レスポンス形式で暗号化している。方向としては、Ｄ（000）からＴ（100）へチャレンジを送信し、Ｔ（100）からＤ（000）へレスポンスを返すという流れである。これをある時間間隔の元に繰り返し、やはり途切れたことを以って、Ｔ（100）が網上に存在しなくなったことを検知している。

以上から、Ｔ（100）が網上に存在しなくなったことをいかにして検知するかが問われているわけだが、この方法に本発明を用いることを提案するものである。

この提案は、通信の方向としてＤ（000）からＴ（100）に対してアクションするという点で、特許文献2に類似する。そのため、特許文献2を引用して、進歩性が否定されるかもしれない。争点は、Ｂの代替物はパスワードと類似するかどうかである。

この点に関しては、基礎となる考え方が全く異なるということを考慮されたい。

第一に、パスワードを発想の基礎においていないこと。本発明によって実現される到達性確認は、そもそも網の特性によって、自動的に得られる値のみで足る。偽装を許容していることからも明らかなように、パスワードに代表される個体識別といった発想ではない。本発明でＢの代替物を許容している理由は答えるべき返事の類型に挙げた通りであって、基本思想に織込まれた、柔軟性を増すための工夫である。それゆえ、パスワードというＤ（000）とＳが一体となっていなければ知ることができないものを根拠にする特許文献2とは、自ずから異なる。

以下に、特許文献２との比較を表に示す。

表05)

	特許文献2	本発明
名称	ヘルスチェック	到達性確認
根拠	パスワード	網の特性 静的な識別子と動的な住所が 関連付けられることによって 到達性が得られる場合に、網の 特性によって、自動的に決まる値)
理論	正規のユーザしか知らないことを 知っているという知識による認証	組A：Bの実像と写像を比較
暗号化	必須 チャレンジ・レスポンス形式	必須ではない ※ してもよい。方式は問わない
柔軟性	バリエーションを許さない	カウンターサインによってキャリアさ れる値はBの代替物であってよい
構造	複雑	単純
セキュリティ上の問題	なりすまし	偽装
影響度	大	小
影響度の判定理由	パスワードを根拠としているため に、なりすまされた場合は、更新 もされうる状態。なお、更新時に は平文パスワードが用いられる	自動的に収束 更新とは、分離されている

表中※印で示した通り、暗号化は必須ではない。根拠や理論から導き出される通り、本来的に答えるべき返事を秘密にする必要はない。

5

答えるべき返事がパスワードでないことは、答えるべき返事は漏洩しても良く、第三者に知られてもかまわないことを意味する。むしろ、アナウンスされた文字列で以って、到達性確認ができるということに特徴を有する。

そして、パスワードでないということは、T (100)において、なんらセキュリティ上の脅威にも結びつ

かない。到達性確認独立の効果でも触れたように、更新と到達性確認は、理論的にも機能的にも、完全に分離されているからである。

それ故、本発明でBそのものがBの代替物に置換あるいは変形された後であっても、特許文献2に比して進歩性を有するものである。

よって、パスワードをベースとして、パスワードの盗聴対策としてチャレンジ・レスポンスを用いた特許文献2とは異なり、網の特性に基づいてより高次の理論（⇐到達性確認）によって単純化し、T（100）が網上に存在しなくなっていることを検知する為にはパスワードをも不要とした。

到達性確認独立の効果は、更にある。

特許文献1に示されたキープアライブを送出するT相当や、特許文献2に示されたヘルスチェックに応答するT相当は、一般的な動的更新端末ではなく、D相当に対する専用の端末にならざるをえないという問題があった。それに対して、本発明のT（100）は独立しているので、専用の端末である必要がない。

この考え方は、網の自律性にそった考え方であるので、D相当とT相当の固定的な関係に束縛される特許文献1や特許文献2と比較して優れている。

ところで、余談であるが、例えばS－1（200）やS－2（300）においても、リソースレコードを消込むことができる。T（100）への到達性が失われたことを、Sは検知することができるので、これをトリガとしてD（000）に対して（消込みの）更新をすればよい。しかし、この場合はT（100）が更新する際に用いるパスワードをS－1（200）やS－2（300）が知っている必要がある。パスワードを知っている人間は、少なければ少ないほど良いのは当然であるので、おススメしない。

なお、この場合の実装であるが、到達性確認の結果が偽であった場合に、図40に開示したシェルスクリプトを実行する等のようにすればよい。図40ではBINDにおけるTSIGを用いた場合の例である。この際、Bそのもの（上記スクリプト例では$TARGETHOST である。この場合はあて先としてのBそのもの）を示すエントリを消す方法とBに対する住所を0.0.0.0やプライベートアドレス等の到達性のない住所に変更する方法がある。上記では前者を採用した。

GNUDIP等のパッケージを用いる場合は、GNUDIPが動作するホストで実施するべきである。この場合、D（000）とGNUDIPが異なるホストで動作していたとしても、一体となっているとみなすべきである。

更新方法については、更新を受付けるホスト上で動作するプログラムに応じて、個別実装されるが

よい。更新過程は、図37のaにいうところのダイヤルアップする機能と連携の取れる方法を用いるべきである。更新処理そのものは従来技術である。D (1000)における消込みの更新のトリガとなる網上におけるT (100)の不存在の検知に到達性確認を用いることができる。

D (1000)がSの機能を実装してする到達性確認の場合には、外部的なホスト間通信としての ②および ③の過程は存在しない。しかし、これはD (1000)が内部的に自分自身に対して、問合せればよいだけである。そのため、比較すべき組A：Bの実像と写像が不十分ということはない。

ダイナミックDNS特有の問題点のまとめ1で、「D (1000)は、T (100)が接続されなくなった後も、最終更新されたリソースレコードをアナウンスし続ける。T (100)からの明示のオフライン処理等がされれば、存在しないT (100)に関する情報をD (1000)がアナウンスし続けることはない。しかし、T (100)の障害時や回線断の際には、オフライン処理をすることができない」と説明した。

ここから、解決すべき課題は、以下のことである。

以下の2つの条件が重なったとき、誤認されたホストT' (200)を発生させる。

T (100)が網上に存在しなくなる。

D (1000)ではT (100)に関する静的な識別子と動的な住所の関連付けが公示されている。（より正確には前記2つの条件が重なったときに、さらに別のホストがダイヤルアップしてくると、それがT' (200)に化けるのだが、ここでは問わない）

この問題を解決するための方法として当初は、T (100)からD (1000)に対してオフライン処理することによって、D (1000)ではT (100)に関する静的な識別子と動的な住所の関連付けを公示しないようにしていた。

歴史的に、T (100)が回線断やT (100)そのものの障害等によってオフライン処理等をすることなく、網上に存在しなくなった場合には、効果がないことが判ってきた。

そこで、D (1000)において、T (100)からのオフライン処理によらずに写像を公示しなくする方法が提案された。その方法における課題は、T (100)が網上に存在しなくなったことを如何にして検知するかであった。曰く、特許文献1では、端末側からDNSへキープアライブ信号を送信することによって、生存していることを通知している。特許文献2は、DNSを用いないながらも、DNS相当側からT相当側に向かってヘルスチェックを行い、T相当が接続されない状態になったことを検出している。

しかし、この方法でもまだ問題が残っている。それはD (1000)は、T (100)がD (1000)に対する専

用の端末でなければ、T (100)が網上に存在しなくなったことを検知することができないことだった。D (000)はT (100)を、D (000) とT (100) との関係の上でのみ成立つ個体識別という考え方によって識別していたために、T (100)が専用の端末であることをD (000)は必須とした。

しかし、この問題も本発明によって解決された。すなわち、本発明によって、専用の端末である必要がなくなったのである。

ダイナミックDNS特有の問題点のまとめ1で指摘した問題点は、実は事象的な問題点であった。すなわち、目に見える問題点である。そしてこれを解決するためには、特許文献1や特許文献2等によるアプローチがあった。すなわち、D (000)の公示が正しくないがゆえに、D (000)の公示を是正しようとするものである。しかし、上記問題点は事象であって、原因は他にある。発明者の洞察に拠れば、その原因は実像と写像の不一致である。従来はSの視点がなかったのだ。この視点によって、SがT (100)への到達性を確認することを実現した。この際Sは、TD間の直接的な関係に依存することなく、T (100) とD (000)からそれぞれ別個に網の構成要件としての4つの要素を得て、その対応の正しさすなわち実像と写像の一致によって、到達性の正しさを確認する。

この考え方に至った時点で、特許文献1や特許文献2のようなD (000)がT (100)を個体識別するという考え方ではなくなっている。そしてこの時点で、到達性確認することのできる通信ノードは、Sである以上あらゆる通信ノードである。それゆえ、本発明によって、専用の端末である必要がなくなったのである。

そしてもちろん、到達性確認は、特許文献1や特許文献2が検知することを目指したT (100)が網上から存在しなくなっている場合をも、検知できるものである。それゆえ当然に、D (000)においても到達性確認をすることはできる。そして、既に挙げたような優位性を有する以上、到達性確認は特許文献1や特許文献2に比して、進歩性を否定されるものではない。本発明は、通信における発信元とあて先がエンド・エンドで到達性確認できるようにしたことに特徴を有する。すなわち、本発明の根幹は到達性確認を実現する理論と実装である。ここでは静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる網にあっては、実像と写像を比較することによって、そのホスト到達性を確認することができるとの、新たな理論を提示した。

この際、カウンターサインという新規のキャリア信号を提案することによって、前記4つの要素のうち、従来では入手することのできなかった要素 (すなわち実像におけるB) を入手することを可能にした。

更なる応用

T 4100)を発信元として、Webサーバ等に接続する際に、Webサーバ側で到達性確認を行うことによって、閉域接続が可能になる。これは情報は公開したいが、誰もが参照できるようにはしたくない等の場合に有効である。例えば、有料課金等の際に、特定のグループを対象にして公開したい場合等である。

手順の1例を以下に挙げる。

手順1。Webサーバ側では、まず特定のグループのメンバとしてT 4100)を登録しておく。このようにして登録されたT 4100)の集合を、データベースと呼ぶ。

手順2。T 4100)からアクセスを受けた際に、到達性確認を行う。ここでは仮にT 4100)は答えるべき返事として、ホスト名 (つまりBそのもの)を返すこととする。

手順3。Webサーバ側では、データベース内から前記得られたホスト名が、合致しているグループを検索する。

手順4。合致したグループに応じたアクセス許可を、発信元であるT 4100)に対して許可する。

手順5。いずれのグループにも合致しなかったT 4100)、到達性確認で偽とされたT 4100)、あるいはT 4100)の機能を実装しない端末からのアクセスの場合には、接続を拒否する。

こうすることによって、閉域接続が可能となる。

この例は、通常あて先として論じられてきたT 4100)を、立場を逆転させてみた。すなわち、答えるべき返事を発信者番号通知として、利用する場合である。

この際、回線交換とは異なり、着信側が自動的に発信者番号を受け取ることができないので、到達性確認によって発信者番号の受け取りに替えるものである。カウンターサインが発信者番号すなわち答えるべき返事を運搬するキャリア信号となる。ここで、例えばIPヘッダにおける発信元住所とは異なる概念であることを示しておく。前記IPヘッダにおける発信元住所は、動的な住所であるところのAであって、静的な識別子であるところのBではない。よって、回線交換でいうところの発信者番号通知に替える機能を持たせる為には、到達性確認が必要なのである。

念の為に記載するが、上記ではWebサーバとしたが、到達性確認に後続する閉域接続することができる処理は、Webサーバのみに制限されるものではない。また、前記手順の2でホスト名としたが、当然にBの代替物であってよい。

なお、TS間において、相互にTの機能とSの機能を実施することもできる。実施例10を参照されたい。こうすることによって、前記した閉域接続の場合よりもさらに閉じた回路をつくることができる。

ところで回線交換の場合は、着信側は発信者番号通知に応じて、選択的に発信元に対して着信を

許可したり拒否したりできる。同様に本発明を応用することによって、T (100)がした答えるべき返事により、SではT (100)からの着信を許可したり拒否したりすることもできる。前記したようにT (100)とSとの立場が逆転していることに注意されたい。このような応用によって、アクセス制御に替えることも可能になる。この方法については、単に閉域接続の逆パターンで足るので、ここまでの説明で容易に想到されるものと考える。

考察)

キャッシュとトラフィックに関する考察

この項は、マッピング公示システムとしてDNSのみがあてはまる。

キャッシュの影響によって発生する誤認を回避する為には、キャッシュを無効化するしかなかった。

キャッシュの機構は、DNSに織り込まれたトラフィックを減ずるための工夫である。したがって、単にキャッシュを無効化すると、トラフィックが増大するおそれがある。

この二律背反を整合する方法を、既に説明してきたものの中から再度2つ挙げて説明する。なお、ここでいうトラフィックはDNSトラフィックのみを指す。したがって、DNSトラフィックのみを減ずることを目的とする。公衆の役務であるDNSについて必要以上に負荷を増大させないことは社会の要請であり、これに応えるものである。TS間のトラフィックは、TS間の通信の頻度に応ずる。

アプリケーション的な解決

通信モデルのシーケンスの最後で、以下のように説明した。

例えば、いったん到達性が確認された後の (2回目以降の)到達性確認においては、 (4) でするサインのあて先であるところのT (100)の住所を記憶しておき、通常は (2)および (3)の過程を省略し、SからT (100)に到達しなくなった時点、すなわち到達性の正しさが確認されなくなった後に、再度 (2)および (3)の過程を実行しても良い。」

この件について、更に説明する。

Sでは到達性が確認された後の、あて先であるT (100)に対する動的な住所を記憶しておき、名前解決や実施例1に示したアドレス確認をするのではなく、このローカルに記憶されたT (100)を示す住所あてに、以後サインを送るようにする。このローカルに記憶をする領域は、Sにおけるアドレス確認の過程で、新たに専用の記憶域を確保するやり方でもよいし、キャッシュをS上に展開してもよい。

前者の新たに専用の記憶域を確保するやり方は、アプリケーションプログラム的な解決方法である。この場合は、T (100)が答えるべき返事として不明な応答を返した時点で、再度実施例1に示すアド

レス確認をすればよい。実施例１に示した２回目のＳ２１６のときに、一定時間待つのではなく、すぐにアドレス確認の過程に戻るようにする。この際、切分の実装にはフラグ等を用いればよい。

これを実装的に説明すると、図示しないが図23で説明すると以下のようになる。

最初に到達性確認に成功した場合をから説明する。

S214の後で、フラグを立てる。既に立っている場合はそのまま。そして、T (100)の住所を記憶して終了する。

次回到達性確認したときは、Ｓ２０２の前で、フラグが立っているかどうかを判断して分岐する。フラグが立っていれば、前記記憶された住所を、S204におけるT (100)を示す住所に代入する。そして、S206から始める。フラグが立っていなければ、通常どおりＳ２０２から始める。

次に到達性確認に失敗した場合である。Ｓ２１６の後で、フラグが立っていればフラグを消す。フラグが元から立っていないない場合はそのまま。Tの住所が記憶されていれば、これも消す。そして、次回到達性確認のタイミングが回ってくるまで待つのではなく、すぐにＳ２０２に戻りやり直す。ただし、この際２回目以降のＳ２１６に該当する場合があるので、一時フラグ等を用いて永久ループを回避するとよい。

フラグの立て方は、ここでは到達性あり (S214) の場合に立てたが、逆 (S216) にしてもよい。この際、当然にS202以前の分岐も逆にする。

後者のキャッシュをＳ上に展開する方法では、キャッシュの生存時間経過後、再度名前問合せをすることになる。もちろん、この場合であっても、T (100)が答えるべき返事として不明な応答を返した場合には、アドレス確認を省略している訳だからすぐさまT (100)は到達しないと判断するべきでなく、アドレス確認からやり直すべきである。

どちらも、名前解決に関するホスト間通信の頻度を減らすことができ、かつキャッシュによる誤認を発生させないようにする効果がある。どちらかというと、前者の方がお勧めである。この理由は、T (100)に到達しなくなるまでの間、名前問合せしないのであるから、結果として名前問合せする頻度が前者の方が少ないことによる。また、Ｓが網接続機器等の比較的資源に余裕がない装置である場合には、キャッシュを展開させるような変更が負担である場合等があり、その際にもアプリケーション的解決の方が有利である。

アプリケーション的解決は、Ｓとして、Ｓ－１ (2000)、Ｓ－２ (300)を許容する。実際的応用に示した第三のフィルタ例D (1000)をＳとする場合と似る。D (1000)をＳとする場合には、名前問合せを省略したのではなく、名前問合せが内部的に完結するので、実質的にホスト間の通信を省略したのと同じことになる。D (1000)とは異なり、内部的な名前解決をすることができないＳ－１ (2000)やＳ－２ (300)

において、正しく到達したT（100）の住所を記憶することによって、内部的な名前解決をさせるようにした。

このようにして、アドレス確認しつつ、ＤＮＳ参照回数を減らし、トラフィックを減ずることができる。

クライアント・サーバ・モデル

クライアント・サーバ・モデルの場合のＳ－２（300）は、不特定多数であってよく、かつＳの機能を実装している必要がない。つまりクライアント・サーバ・モデルを採用する理由は、Ｓの機能を実装しない既存の通信ノードに対して、到達性確認というサービスを提供できるようにするものである。しかし、クライアント・サーバ・モデルを採用するもうひとつの理由がある。

集約効果である。

これは図で説明すると判り易い。

図41（a）にピア・トゥ・ピア・モデルを採用した場合を示す。ピア・トゥ・ピアの場合は、Ｓ－１（2000）とＳ－２（300）はいずれであってもよい。そのため図中のＳ－２（300）はＳ－１（2000）と読替えてもよい。

図41（b）にクライアント・サーバ・モデルを採用した場合を示す。

図41（a）の場合であって、仮にあらゆる端末がＳ－２（300）になる場合を考えると、クライアント・サーバ・モデルの必要性は明らかである。これがエンド・エンドで到達性確認できるにもかかわらず、クライアント・サーバ・モデルを提案した理由である。

従来からいわれているように、ピア・トゥ・ピア・モデルが小規模通信向け、クライアント・サーバ・モデルが大規模通信向けと考えればよい。

クライアント・サーバ・モデルは名前問合せに係るトラフィックを減ずるだけのための工夫ではないが、キャッシュの無効化とトラフィックの増大の関係を整合することに貢献する。

哲学的な考察

発明の過程において発明者は、認証とは、網上におけるホストとヒトの違いは何かと考えていた。

ヒトは網上では、ホストの向こう側にいる存在であった。すなわち、レイヤが違う。そんなことは、わかっているのだ。しかし、どうも明確にヒトとホストを分かつ境界が見えないのであった。

そこで、以下のように考えることにした。

人間の認証がパスワードである。ホストは、X509証明書や、IPSec認証ヘッダ等によって、認証することができる。そして、機械（通信ノード）の網上での到達性確認がサイン・アンド・カウンターサイン

である。その意味で、人間の認証、ホストの認証と、ホストの到達性確認は並立する概念である。ここで、機械（通信ノード）の到達性確認とは、特別の許可ではないという点で認証より緩やかな概念（例：アクセス権の許可ではない）であって、通信の相手方として、正しい相手方であることを確認する過程である。

以上によって、従来の端末認証等の個体識別という概念によらず、網の特性によって網上の通信相手を確認する方法を提案した。

（今後の課題）

課題１

S－１（2000）やS－２（3300）において、以下の条件が重なった時に、本発明は効果がない。

条件１　T（4100）が網上に存在しない。

条件２　D（1000）において、T（4100）に対する組A：Bの写像を公示。（この場合、T（4100）が存在しない以上、Aに誤りがある。そして、D（1000）においてSの機能を実施し、T（4100）を示す写像の消込みもされていない。）

条件３　T’（4200）が網上に存在しない。（つまり、誤認も発生していない）

以上の条件が重なった時には、SからT（4100）への通常の通信と同様、到達性確認もまた、単にタイムアウトするまで待つという点で、到達性をあえて確認する利益がない。

課題２

処理を含む各過程に対して、インターフェースの標準化をした方がよい。

本明細書による開示では、各構成要素（特にS）における後続する処理については、個別実装とした。後続する処理は従来技術である。本明細書の開示のみでは本発明と従来技術の接続点に関して、個別に作り込まなければならない。

そこで、各処理におけるやり取りを規定することによって、到達性確認をモジュール化することができる。

プログラム間インターフェースを標準化するという提案である。

インターフェースが標準化されれば、例えばSで動作するプログラムをマネージャ、T（4100）で動作するプログラムをエージェントとする等によって、更に理論化できる。

インターフェースを標準化することによって、個別の作り込みをするのでなく、

ちょうどリゾルバがありとあらゆる通信アプリケーションソフトの前置処理として動作するように、本

発明もあらゆるプログラムの前置処理として動作させることができる」ようになる。

課題３

カウンターサインの用いる通信ポートに関しても、標準化をした方がよい。

用語の説明）

以下に、本文中で説明できなかった重要な用語について説明する。

暗号化とは：

あるルールに従ってオリジナルの文字列を変形したものであって、復号化が必要なもの。ここでは目的は問わない。すなわち必ずしも秘密の漏洩を防ぐことを目的としない場合がある。例えば、通信路そのものやディスクそのものが暗号化されている場合には、暗号化された情報のうちには、秘密にする必要のあったものは本のわずかであって、その大半は秘密にする必要がなかったものかもしれない。あるいは秘密にする必要のないものしか含まれていないこともあり得る。この際、秘密にする必要のなかった情報が暗号化された目的は、秘密の漏洩を防ぐことではない。秘密にする必要があるかないかは、情報の質の問題である。本発明において、Ｔが答えるべき返事が、仮にＢの変形である場合であっても、そもそもＢそのものが秘密にする必要のない情報であるので、秘密の漏洩を防ぐことを目的とするとはいえない。本文中で触れたように、基本思想に織込まれた、柔軟性を増すための工夫である。

認証とは：

認証とは、正規利用者本人だと確認する過程。例えば、システムにログインする権利の確認あるいはファイルシステムへのアクセス権を獲得する過程。

パスワードとは：

暗号化とは異なる概念であって、何らルールに基づかず、また復号を必要としない、単に秘密の文字列であって、認証の為に用いるもの。

これは、暗号化パスワードと平文パスワードが区別されることからも明らかである。パスワードは、知識による認証とよばれるものに属し、ユーザＩＤに対応するパスワードを知っているという事実を以って、そのユーザが正規の利用者であるという判断をするものである。すなわち、本人を正しく特定できることを目的としている。パスワードは、通常個体識別名とともに、個体識別に用いる。すなわち、認証とパスワードはともに、個体識別をベースとして発想されたものである。

ところで、チャレンジ・レスポンス形式によって暗号化されたパスワードやＳ／ＫＥＹ等のワンタイム

パスワードも、ここではパスワードに含めて考える。

また、ＤＮＳの場合であって、更新に用いるパスワードには、便宜上ＴＳＩＧ(RFC2845)を含めて考えている。これは、Ｔ(100)とＤ(000)において秘密鍵を共有することから、知識による認証に準ずるものと考えて差し支えないからである。

・ホストとは：

端末、ルータ等を含む、住所を割当てられた通信ノードすべて。よって、本発明では、ホストという用語には、計算機のみでなくゲートウェイをも含むものとする。

・ゲートウェイとは：

アプリケーションゲートウェイのみをゲートウェイとする説があるが、本明細書ではルータ、アプリケーションゲートウェイ、プロトコル変換装置等のIP的網境界を構成するものを総称する。

・カスタマとは：

Ｔ(100)の所有者のこと。カスタマ網とは、Ｔ(100)の所有者が管理する網であって、公共の網でないもの。

・リゾルバとは：

ＤＮＳに対して名前問合せをする機能のこと。ＤＮＳから見れば名前問合せをしてくるものである。

本発明で多用される技術以外の重要な概念について定義する。

・代替とは：

他のもので代えること※

・集合とは：

一定の範囲にあるものを一つの全体として考えたもの※

本発明では、この一定の範囲とは、特定の機能を代替し得るものと考える。さらに独立した機能が集合することによって、上位の機能を形成する場合もこれに含む。

・代表とは：

団体の中から選ばれ、その団体の意見や意志を反映する者として他との交渉に当たる・こと※

その一つを取り出しただけで全体の特徴が概観できる・こと(もの)※

・典型とは：

特定の集合の中で最も特徴的であるか、目立つものをいう。

したがって、集合の持つ性質を、正確に反映している訳ではない。

・一体となった場合とは：

一の具体的な装置において、複数の機能が複合した場合をいう。

関連付けとは：

マッピング公示システムによって対応付けられる、静的な識別子と動的な住所は、本来的には1対1に対応付けられるべきものである。しかし、1対1でない場合があることや、中間識別子である場合等を考慮して、静的な識別子と動的な住所は関連付けられるものとした。

なお、※印あるものについては、新明解国語辞典を引用した。

その他の用語については一般的な、もしくは当業者の技術常識にしたがって解釈されたい。

図面の簡単な説明)

図01 Tもしくはカスタマ網において、ダイヤルアップを示す図である。

図02 Tもしくはカスタマ網において、アドレス割当てを示す図である。

図03 Tもしくはカスタマ網において、ＤＮＳ更新を示す図である。

図04 Tもしくはカスタマ網において、正常状態を示す図である。

図05 Tもしくはカスタマ網において、回線断発生を示す図である。

図06 Tもしくはカスタマ網において、再接続を示す図である。

図07 Tもしくはカスタマ網において、アドレス割当て 再)を示す図である。

図08 Tもしくはカスタマ網において、ＤＮＳ更新 再)を示す図である。

図09 Tもしくはカスタマ網において、ホストがすり替わっているように見える状態を示す図である。

図10 各網において、参照されるＤＮＳを示す図である。

図11 Tもしくはカスタマ網において、誤認を示す図である。

図12 Tもしくはカスタマ網において、正常状態 収束)を示す図である。

図13 Tもしくはカスタマ網において、回線断のまま 図06以降の別パターン)を示す図である。

図14 Tもしくはカスタマ網において、回線断のままの場合の誤認、亦は第二の保守経路による保守を示す図である。

図15 TとＤの対応状況を示す図である。

図16 Tを正引き名前問合せする場合において、キャッシュが有効な時のＤＮＳの探索順を示す図である。

図17 Tを正引き名前問合せする場合において、キャッシュが有効でない時のＤＮＳの探索順を示す図である。

図18 キャッシュの生存時間を示す図である。

図19 キャッシュの生存時間の収束1（計測プログラム）を示す図である。

図20 キャッシュの生存時間の収束2（計測結果1）を示す図である。

図21 キャッシュの生存時間の収束4（計測結果2の続き）を示す図である。

図22 通信モデルを示す図である。

図23 課題を解決するための手段を示すフローチャートである。

図24 課題を解決するための手段2（S204のオプション処理）を示すフローチャートである。

図25 DIGコマンド正常出力例を示す図である。

図26 DIGコマンドエラー出力例（DNSサーバが存在しない場合）を示す図である。

図27 DIGコマンドエラー出力例（Tが存在しない場合）を示す図である。

図28 SNMP正常出力例（Iが正しい到達性の場合）を示す図である。

図29 SNMPエラー出力例（ホストが間違いの場合）を示す図である。

図30 SNMPエラー出力例（コミュニティ名が間違いの場合）を示す図である。

図31 SNMPエラー出力例（オブジェクトIDの指定間違いの場合）を示す図である。

図32 BINDにおけるバージョン情報の設定の為にする設定ファイルの変更箇所を示す図である。

図33 DIGコマンド正常出力例を示す図である。

図34 DIGコマンドエラー出力例（Tが存在しなかった場合）を示す図である。

図35 DIGコマンドエラー出力例（別のネームサーバを参照してしまった場合）を示す図である。なお、バージョン情報が設定されていない場合の標準的な出力例（正常）でもある。

図36 SMTPサーバ（SENDMAIL）に接続した際の最初のメッセージ例を示す図である。

図37 Tのカスタマ網における接続形態を示す図である。

図38 各ホストと網の位置関係を示す図である。

図39 本発明をいわゆるping代替として用いる場合の動作の違いを示す図である。

図40 DNS更新スクリプト・サンプルを示す図である。

図41 クライアント・サーバ・モデルにおける集約効果を示す図である。

符号の説明）

記号　名称

1000　D。マッピング公示システムである。DNSが代表例であるが、DNSのみを指す訳ではなく特許文献2の場合等も含む。DNSと表記された場合には、DNSのみを指す場合と、DNSでないが

組A：Bの写像を公示するものである場合がある。

2000　S－1。発信元管理サーバである。S－2（300）とあわせて、発信元であるSという概念に抽象化される。この際、発信元とは、Tへの到達性の正しさを確認しようとするものである。

4000　P。管理対象機器の接続先たるプロバイダである。あるいはカスタマ網から見て上流の網（DNSサーバ等がある側）を構成し、これに接続される網境界ノードに住所を動的に割当てる機能を有する網を指す。DHCPサーバ、そしてDHCPサーバと管理対象機器を含む網を許容する。

4100　T。網に対して、断続的に接続および切断（移動亦は携帯を含む）を繰返すダイヤルアップのホストであって、あて先たる管理対象機器である。

4200　T'。プロバイダPの別のユーザ。プロバイダPから住所の割当てを受けるユーザ（亦はホスト）であって、管理対象機器でないユーザである。管理対象機器がかつて割当を受けていた住所を割当てられる可能性があるという点で、管理対象機器と誤認されるおそれのあるホストのこと。

4500　P－D。プロバイダPのDNSサーバ。

5000　P－2。プロバイダPでないプロバイダである。管理対象機器の接続先以外のプロバイダ。すなわちインターネットの一般利用者（300）の接続先たるプロバイダである。この概念はプロバイダPがインターネットに接続しているかもしくはプロバイダPがその他の網と相互接続されている場合にのみ有効な考え方である。

5300　S－2（300）。一般利用者たる発信元である。インターネットの一般利用者（300）。管理サーバやDNSの管理者および管理対象機器の運用者、管理対象機器の直接利用者（閲覧者を除く）から見た、第三者のことである（管理対象機器に対する閲覧者は、一般利用者に当たる）。管理対象機器（あるいはカスタマ網とプロバイダPの網境界）に住所を動的に割当てるプロバイダPがインターネットに接続しておりかつプロバイダP－2がインターネットに接続しているか、もしくはプロバイダPとプロバイダP－2が相互接続されている場合にのみ一般利用者（300）の概念は（管理対象機器から見て）プロバイダP－2の上で成立する。すなわち、プロバイダP－2は（プロバイダPから見て）ルーティングによって到達する別の網でありさえすればよい。管理対象機器に対して通信を始めようとするノードである。

5500　P－2－D。プロバイダP－2のDNSサーバ

請求の範囲

1 静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる蓄積交換網において、

マッピング公示システム（000）における被到達性確認通信ノード（100）を示す静的な識別子と動的な住所からなる組の写像と、

被到達性確認通信ノード（100）における静的な識別子と動的な住所からなる組の実像とを比較することによって、

被到達性確認通信ノード（100）への到達性の真偽を判定することを特徴とする通信モデル。

2 請求項1の通信モデルにあって、

以下のシーケンスによって、前記通信モデルにおける比較する要素のすべてを到達性確認通信ノード（000）が知る手順。

(1) 到達性確認通信ノード（000）は被到達性確認通信ノード（100）の静的な識別子をキーにマッピング公示システムに対して要求する名前問合せ。

(2) マッピング公示システムは、この問合せに対して被到達性確認通信ノード（100）の動的な住所を応答する名前解決。

(3)到達性確認通信ノード（000）は前記応答された被到達性確認通信ノード（100）を示す動的な住所あてに単に応答することを要求するサイン。

(4) 被到達性確認通信ノード（100）が答えるべき返事を新規のキャリア信号に載せて応答するカウンターサイン。

3 請求項1に記載の通信モデルにおいて、

被到達性確認通信ノード（100）が到達性確認通信ノード（000）に到達性を確認させる情報を搬送することを特徴とする信号。

4 請求項3に記載の信号において、

被到達性確認通信ノード（100）が到達性確認通信ノード（000）に到達性を確認させる情報が、被到達性確認通信ノード（100）が答えるべき返事である情報を搬送することを特徴とする信号。

5 請求項3に記載の信号において、

被到達性確認通信ノード(100)が到達性確認通信ノード(200)に到達性を確認させる情報が、被到達性確認通信ノード(100)が答えるべき返事である情報に加えて、さらに附加情報を搬送することを特徴とする信号。

6 被到達性確認通信ノード(100)において、到達性確認通信ノード(200)からの応答要求に応じてする応答において、答えるべき返事をキャリーする機能を有するキャリア信号。

7 請求項6に記載の信号において、答えるべき返事に加えてさらに附加情報をキャリーすること機能を有するキャリア信号。

8 静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる蓄積交換網において、

到達性確認通信ノード(200)に任意の情報を被到達性確認通信ノード(100)への到達性を確認させる情報として記憶させ、到達性確認通信ノード(200)と被到達性確認通信ノード(100)とが所定の通信をすることによって被到達性確認通信ノード(100)が到達性確認通信ノード(200)に対してした返信を前記記憶した情報と比較することによって、被到達性確認通信ノード(100)への到達性を到達性確認通信ノード(200)に確認させることを特徴とする到達性確認の方法。

9 請求項8に記載された到達性確認の方法において、

任意の情報が、被到達性確認通信ノード(100)における静的な識別子であることを特徴とする到達性確認の方法。

10 請求項8に記載された到達性確認の方法において、

任意の情報が、被到達性確認通信ノード(100)と関連づけられていることを到達性確認通信ノード(200)が知っている場合に静的な識別子に置き換えられたあらゆる文字列であることを特徴とする到達性確認の方法。

11 請求項8に記載された到達性確認の方法において、

任意の情報が、被到達性確認通信ノード(100)と関連づけられていることを到達性確認通信ノード

2000)が知っている場合に静的な識別子に替わって使用される変形ルールであることを特徴とする到達性確認の方法。

12 請求項8に記載の到達性確認の方法において、

被到達性確認通信ノード4100)において、被到達性確認通信ノード4100)の記憶装置に任意の情報を答えるべき返事として保存し、あらかじめ合意された方式での通信に対して前記保存された情報を記憶装置より読み出し、少なくとも該情報を含めたカウンターサインを返信することによって、被到達性確認通信ノード4100)が到達性の被到達性確認通信ノード4100)であることを到達性確認通信ノード 2000)に確認させることを特徴とする到達性確認の方法。

13 請求項8に記載の到達性確認の方法において、

被到達性確認通信ノード4100)の静的な識別子を管理する複数存在するマッピング公示システム 1000)の内の1のマッピング公示システム 1000)を選択して正引き名前問合せをして、参照する被到達性確認通信ノード4100)毎に異なるマッピング公示システム 1000)に切り替えることによって、被到達性確認通信ノード4100)の動的な住所を取得して、請求項8に記載の被到達性確認通信ノード4100) と前記所定の通信をするために前記取得した動的な住所を用いておこなうことを特徴とする到達性確認の方法。

14 請求項8から請求項13のいずれかに記載の到達性確認の方法において、

被到達性確認通信ノード4100)への到達性確認に失敗した場合に、所定の時間間隔を経過した後、再度請求項8から請求項13のいずれかに記載の到達性確認の方法を実施することによって、被到達性確認通信ノード4100)に対する到達性の真偽を確認することを特徴とする到達性確認の方法。

15 請求項8から請求項14のいずれかに記載の到達性確認の方法において、到達性確認通信ノード2000)が到達性を確認する機能を有しない端末に替わってする到達性確認の方法

16 請求項8から請求項14のいずれかに記載の到達性確認の方法において、

前記到達性確認の結果を、所定の対象者または公衆に通知することをさらに具備することを特徴とする到達性確認の方法。

17 請求項8から請求項16のいずれかに記載の到達性確認の方法において、到達性確認通信ノード(2000)が到達性確認する機能を有しない端末からの被到達性確認通信ノード(4100)に対する到達性確認要求を受け、到達性確認通信ノード(2000)が被到達性確認通信ノード(4100)に対する到達性の真偽を確認し、その結果を到達性確認する機能を有しない端末に応答することを特徴とする到達性確認の方法。

18 請求項17に記載の到達性確認の方法において、到達性確認の結果を到達性確認する機能を有しない端末に応答する際に、さらに到達性確認する機能を有しない端末がキャッシュの影響を受ける時間を予測して、正常にアクセスできる時間を更に前記応答に含めることを特徴とする到達性確認の方法。

19 SNMPマネージャを用いてする到達性確認の方法に先だって、請求項8から請求項14のいずれかに記載の被到達性確認通信ノード(4100)への到達性確認を実施し、ここで被到達性確認通信ノード(4100)の到達性が確認された場合に、到達性が確認された被到達性確認通信ノード(4100)の動的な住所を、SNMPマネージャを用いてする到達性確認の方法に引き渡すことによって、動的に住所が変化する被到達性確認通信ノード(4100)を管理することを特徴とする到達性確認の方法。

20 請求項8から請求項14のいずれかに記載の到達性確認の方法において、到達性確認することによって、被到達性確認通信ノード(4100)が網上に存在しないことが検知された場合に、マッピング公示システムが公示する被到達性確認通信ノード(4100)に関する静的な識別子と動的な住所の関連付けを公示しないようにマッピング公示システムを構成しなおす方法。

21 請求項20に記載の到達性確認の方法において、到達性確認することによって、被到達性確認通信ノード(4100)が網上に存在しないことが検知された場合に、被到達性確認通信ノード(4100)の属するドメイン名を管理するDNSサーバにおいて、被到達性確認通信ノード(4100)に関するリソースレコードの消込みをする方法。

22 請求項8から請求項14のいずれかに記載の到達性確認の方法を用いて、蓄積交換網において発信者番号通知する方法。

23 請求項22に記載の方法を用いてする閉域接続する方法。

24 請求項8から請求項14のいずれかに記載の到達性確認の方法において、被到達性確認通信ノード(100)に関する到達性の確認が取れた住所を到達性確認通信ノード(2000)が記憶することによって、DNSに対する名前解決過程を省略し、このことによって、DNSトラフィックを減ずる方法。

25 請求項8から請求項14のいずれかに記載の到達性確認の方法において、
到達性確認の結果を次の処理の入力として用いるあらゆるプログラム。

26 請求項8から請求項24のいずれかに記載の到達性確認の方法を、
計算機もしくはネットワーク接続機器に実行させるためのプログラム。

27 計算機もしくはネットワーク接続機器であって、
該装置に被到達性確認通信ノード(100)毎に少なくともサインが設定され、答えられるべき返事が被到達性確認通信ノード(100)を示す静的な識別子そのものでない場合には答えられるべき返事をも設定され、該装置から被到達性確認通信ノード(100)にサインを送信する手段と、被到達性確認通信ノード(100)から応答されるカウンターサインを受信する手段と、前記受信されたカウンターサインによって搬送された答えるべき返事と前記設定された答えられるべき返事とを比較する手段とを備え、比較された結果の真偽によって被到達性確認通信ノード(100)に対する到達性の真偽を確認することを特徴とする通信ノード。

28 請求項27に記載の通信ノードにおいて、
被到達性確認通信ノード(100)の使用する静的な識別子を管理する複数存在するマッピング公示システム(1000)の内の1のマッピング公示システム(1000)を、被到達性確認通信ノード(100)毎に選択して逆引き名前問合せをして、被到達性確認通信ノード(100)の動的な住所を取得して、被到達性確認通信ノード(100)と通信するために前記取得した動的な住所を用いておこなうことを特徴とする通信ノード。

29 請求項27から請求項28のいずれかに記載の通信ノードにおいて、

被到達性確認通信ノード4100)への到達性確認に失敗した場合に、所定の時間間隔を経過した後、再度請求項27に記載の到達性確認を再度実施することによって、正しい到達性の被到達性確認通信ノード 4100)に到達するか否かを確認することを特徴とする通信ノード。

30 請求項27から請求項29のいずれかに記載の通信ノードにおいて、

一般利用者の使用する通信ノードからの要求に応じて、前記到達性確認をすることを特徴とする通信ノード。

31 請求項27から請求項30のいずれかに記載の通信ノードにおいて、

前記到達性確認の結果を、所定の対象者または公衆に通知することをさらに具備することを特徴とする装置。

32 請求項27から請求項31のいずれかに記載の通信ノードにおいて、

到達性確認する機能を有しない端末からの被到達性確認通信ノード 4100)に対する到達性確認要求を受け、到達性確認通信ノード2000)が被到達性確認通信ノード4100)に対する到達性の真偽を確認し、その結果を到達性確認する機能を有しない端末に応答することを特徴とする通信ノード。

33 請求項32に記載の通信ノードにおいて、

到達性確認の結果を到達性確認する機能を有しない端末に応答する際に、さらに到達性確認する機能を有しない端末がキャッシュの影響を受ける時間を予測して、正常にアクセスできる時間を更に前記応答に含めることを特徴とする通信ノード。

34 請求項27から請求項31のいずれかに記載の到達性確認に後続して、ＳＮＭＰマネージャを用いてする到達性確認の方法に接続するために、

請求項27から請求項31のいずれかに記載された到達性が確認された被到達性確認通信ノード4100)の動的な住所を、ＳＮＭＰマネージャを用いてする到達性確認の方法に引き渡すことによって動的な住所が変化する被到達性確認通信ノード4100)を管理することを特徴とする通信ノード。

35 請求項27から請求項29のいずれかに記載の通信ノードにおいて、

到達性確認することによって、被到達性確認通信ノード（100）の網上における不存在を検知したときに、マッピング公示システム（1000）における被到達性確認通信ノード（100）を示す静的な識別子と動的な住所からなる組の写像の公示を公示しないように変更するマッピング公示システム（1000）。

36 請求項35に記載のマッピング公示システム（1000）において、

到達性確認することによって、被到達性確認通信ノード（100）が網上に存在しないことが検知された場合に、被到達性確認通信ノード（100）の属するドメイン名を管理するＤＮＳサーバにおいて、被到達性確認通信ノード（100）に関するリソースレコードの消込みをするＤＮＳサーバ。

37 請求項27から請求項29のいずれかに記載の通信ノードにおいて、

カウンターサインによってキャリーされた、蓄積交換網における発信者番号通知を受信する通信ノード。

38 請求項37に記載の通信ノードにおいて、

事前に設定された発信者番号を通知する通信ノードのみに対して、所定のサービスを提供する通信ノード。

39 請求項27から請求項29のいずれかに記載の通信ノードにおいて、

被到達性確認通信ノード（100）に関する到達性の確認が取れた住所を記憶することによって、ＤＮＳに対する名前解決過程を省略した到達性確認通信ノード（2000）。

40 請求項27から請求項39のいずれかに記載の通信ノードにおいて、

通信ノードの機能が、複数の装置によって共有されることからなるセンタ側のシステム。

41 請求項27から請求項39のいずれかに記載の通信ノードにおいて、

計算機もしくはネットワーク接続機器に実行させるためのプログラム。

42 計算機もしくはネットワーク接続機器であって、

住所の割当てを動的に受けてなる通信ノードもしくは外部ネットワークからは該通信ノードと一体となって参照される通信ノードのいずれかであって、

該通信ノードの記憶装置に任意の情報を答えるべき返事として保存し、サインもしくはあらかじめ合意された方式での通信に対して前記保存された情報を該記憶装置より読み出し、少なくとも該情報を含めたカウンターサインもしくはあらかじめ合意された方式での通信に対するカウンターサインを返信するように構成されることを特徴とする通信ノード。

43 請求項42に記載の通信ノードにおいて、

該通信ノードにおいて保存された答えるべき返事が到達性確認通信ノード(2000)に対して事前に通知されていること条件として、あらゆる文字列で以って設定されるものであって、該文字列が該通信ノードの記憶装置に保存され、所定のポートへの通信要求を受けた際に、前記保存された文字列を該記憶装置より読み出し、少なくとも該文字列を含めた返信をするように構成されることを特徴とする通信ノード。

44 請求項42に記載の通信ノードにおいて、

該通信ノードにはホスト名が設定されるものであって、該ホスト名が該通信ノードの記憶装置に保存され、所定のポートへの通信要求を受けた際に、前記保存されたホスト名を該記憶装置より読み出し、少なくとも該ホスト名を含めた文字列を返信するように構成されることを特徴とする通信ノード。

45 請求項42に記載の通信ノードにおいて、

ダイナミックDNSによって動的更新されるセンタ側マッピング公示システム(1000)において設定されるホスト名をFQDNでもって、該通信ノードに読み出し可能な文字列として設定されるものであって、該文字列が該通信ノードの記憶装置に保存され、所定のポートへの通信要求を受けた際に、前記保存された文字列を該記憶装置より読み出し、少なくとも該文字列を含めた文字列を返信するように構成されることを特徴とする通信ノード。

46 請求項42から請求項45のいずれかに記載の通信ノードにおいて、

請求項42から請求項45のいずれかに記載の待受けされる所定のポート以外に、該通信ノードの設定変更用のポートあるいは、一般の閲覧に供するためのウェブサービスを提供するウェルノウンなポートのいずれかのポート、あるいはその両方のポートで待受けされる所定のポートを備えるように構成されることを特徴とする通信ノード。

47 請求項42から請求項46のいずれかに記載の通信ノードにおいて、

到達性確認通信ノード(2000)からのサインもしくはあらかじめ合意された方式での通信に対して、

被到達性確認通信ノード(4100)がカウンターサインもしくはあらかじめ合意された方式での通信に対するカウンターサインを返信することによって、

到達性確認通信ノード(2000)に、被到達性確認通信ノード(4100)への到達性を判定させることを特徴とする通信ノード。

48 請求項42から請求項47のいずれかに記載の通信ノードにおいて、

答えるべき返事をキャリーするキャリア信号をサインに応答して送出することを特徴とする通信ノード。

49 請求項49に記載の通信ノードにおいて、

答えるべき返事として自己の識別情報をキャリーするキャリア信号をサインに応答して送出することを特徴とする通信ノード。

50 請求項49に記載の通信ノードにおいて、

前記キャリア信号をサインに応答して送出することによって、発信者番号通知に替えることを特徴とする通信ノード。

51 請求項42から請求項50のいずれかに記載の通信ノードとしての機能を、

計算機もしくはネットワーク接続機器に実現させるためのプログラム。

図０１

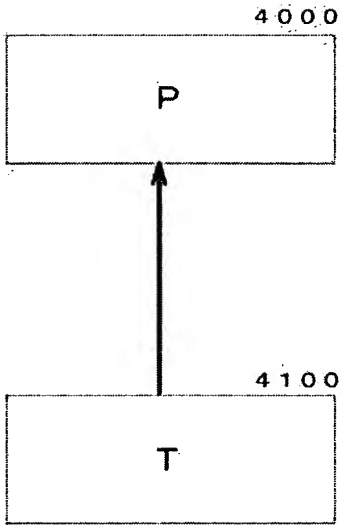


図０２

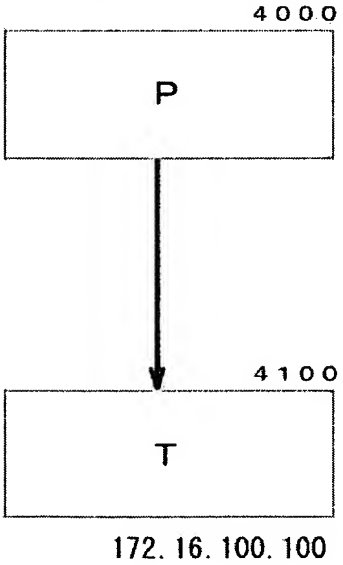


図０３

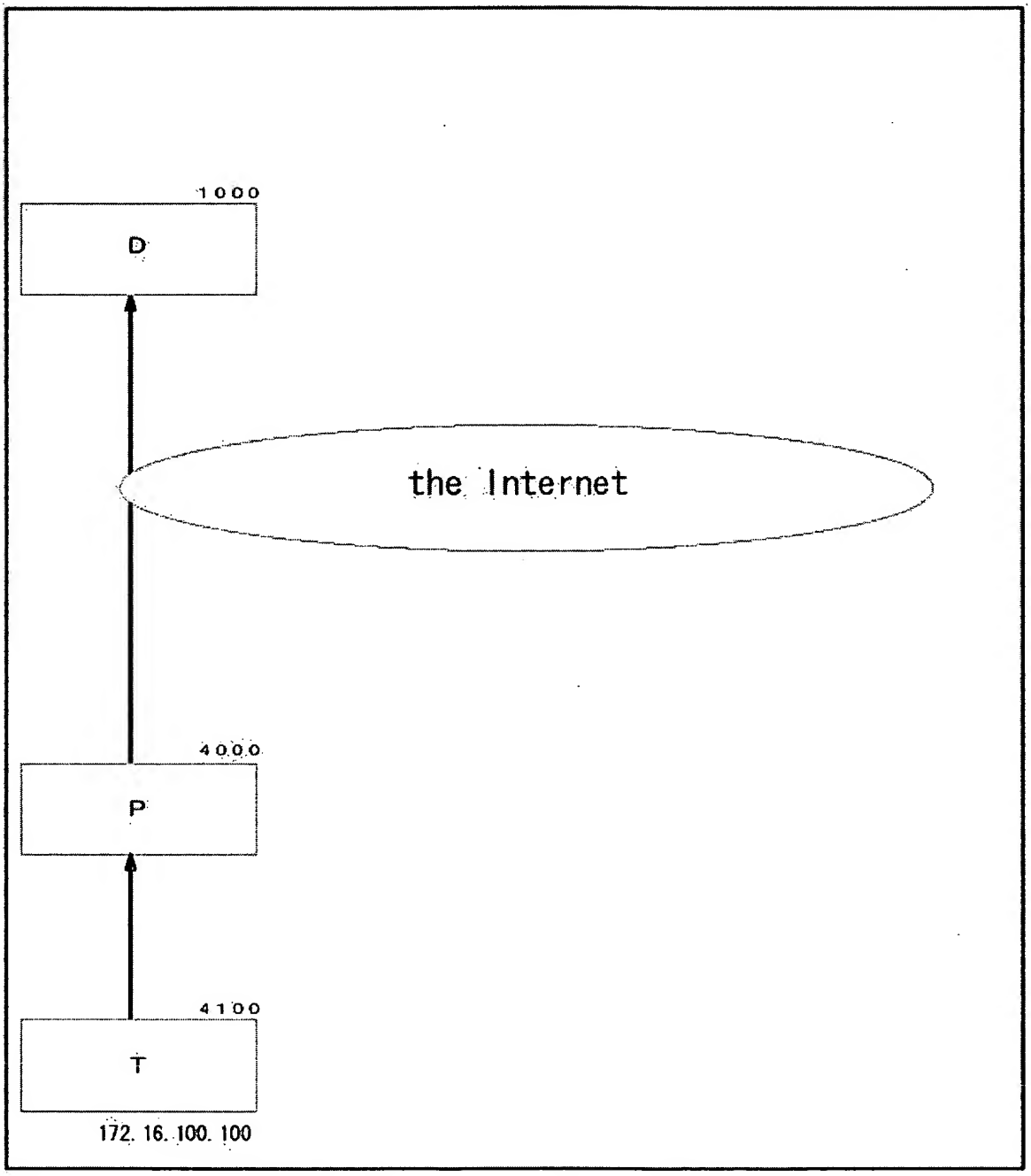


図０４

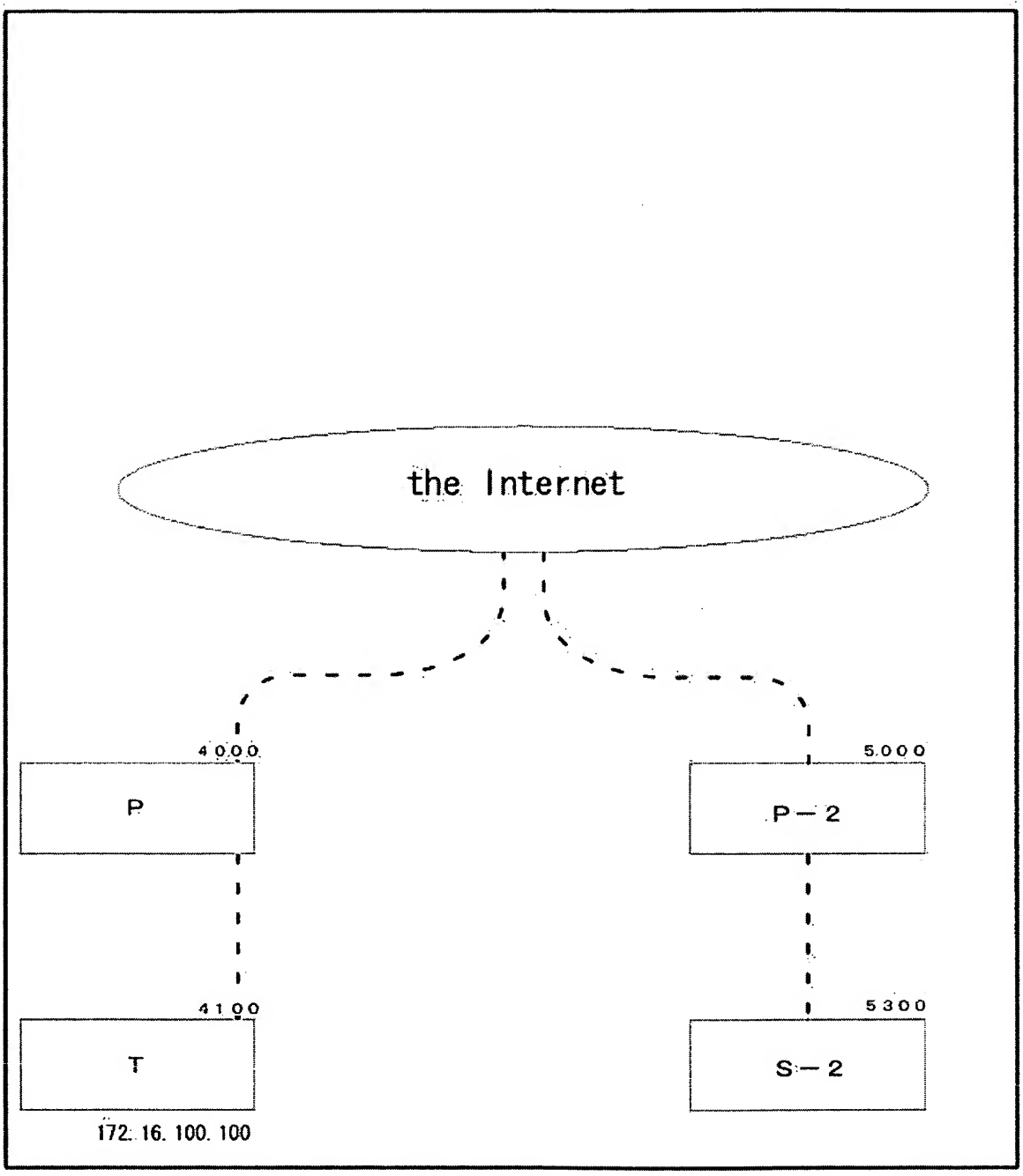


図０５

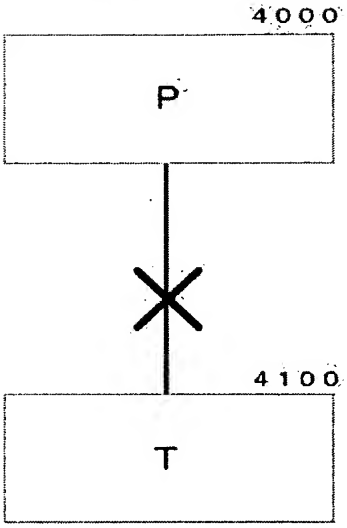


図０６

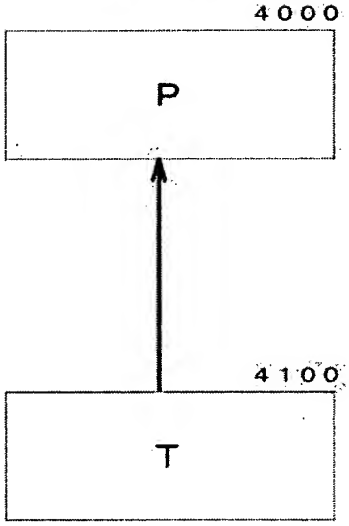
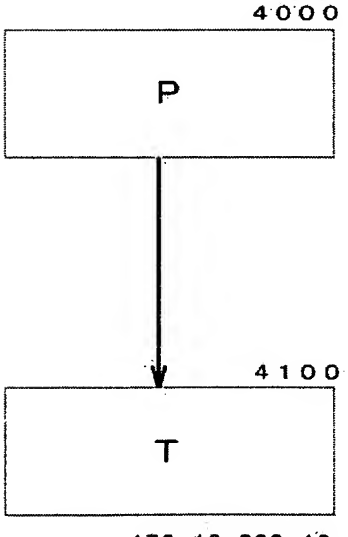


図０７



172. 16. 200. 10

図０８

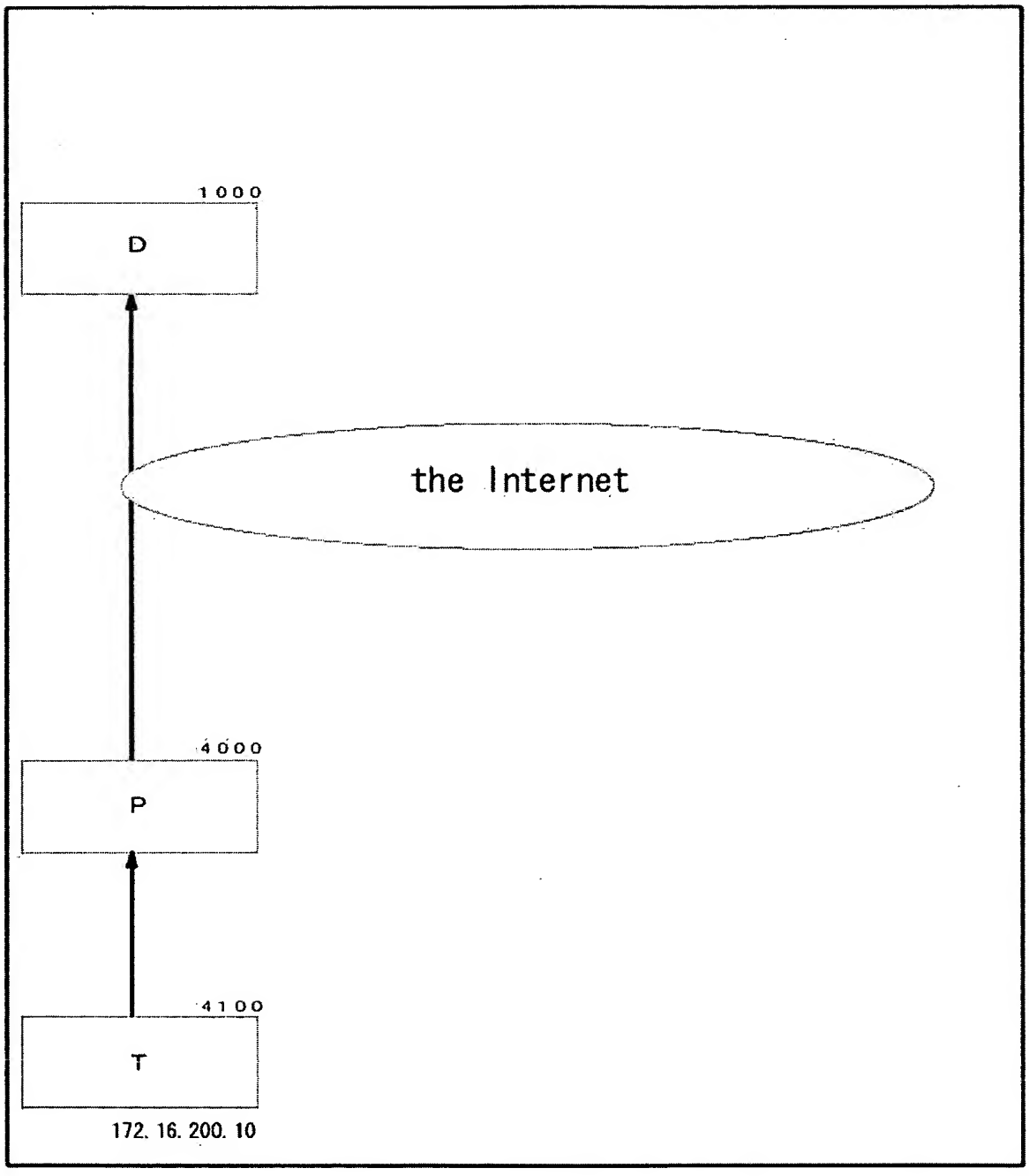


図０９

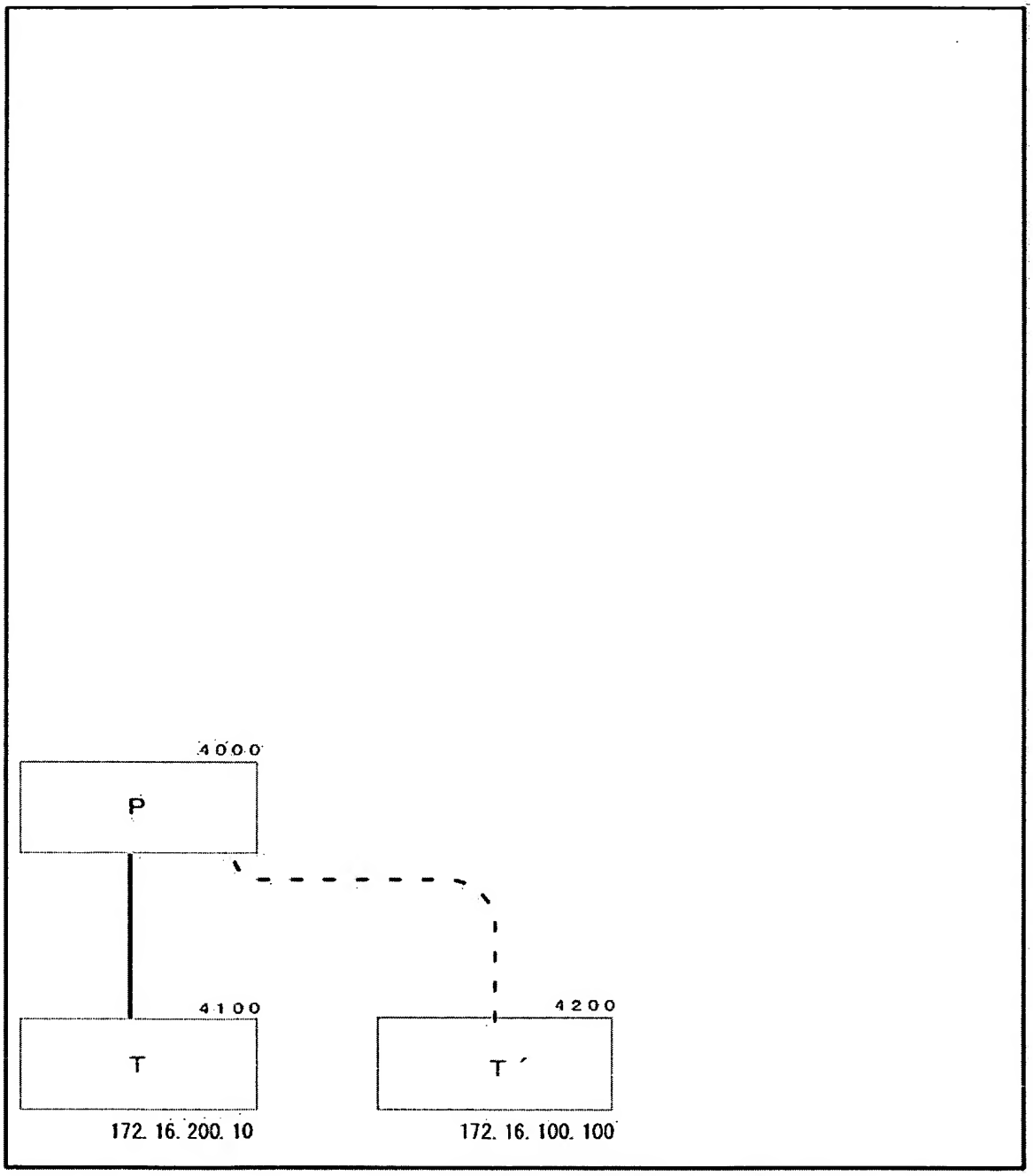


図１０

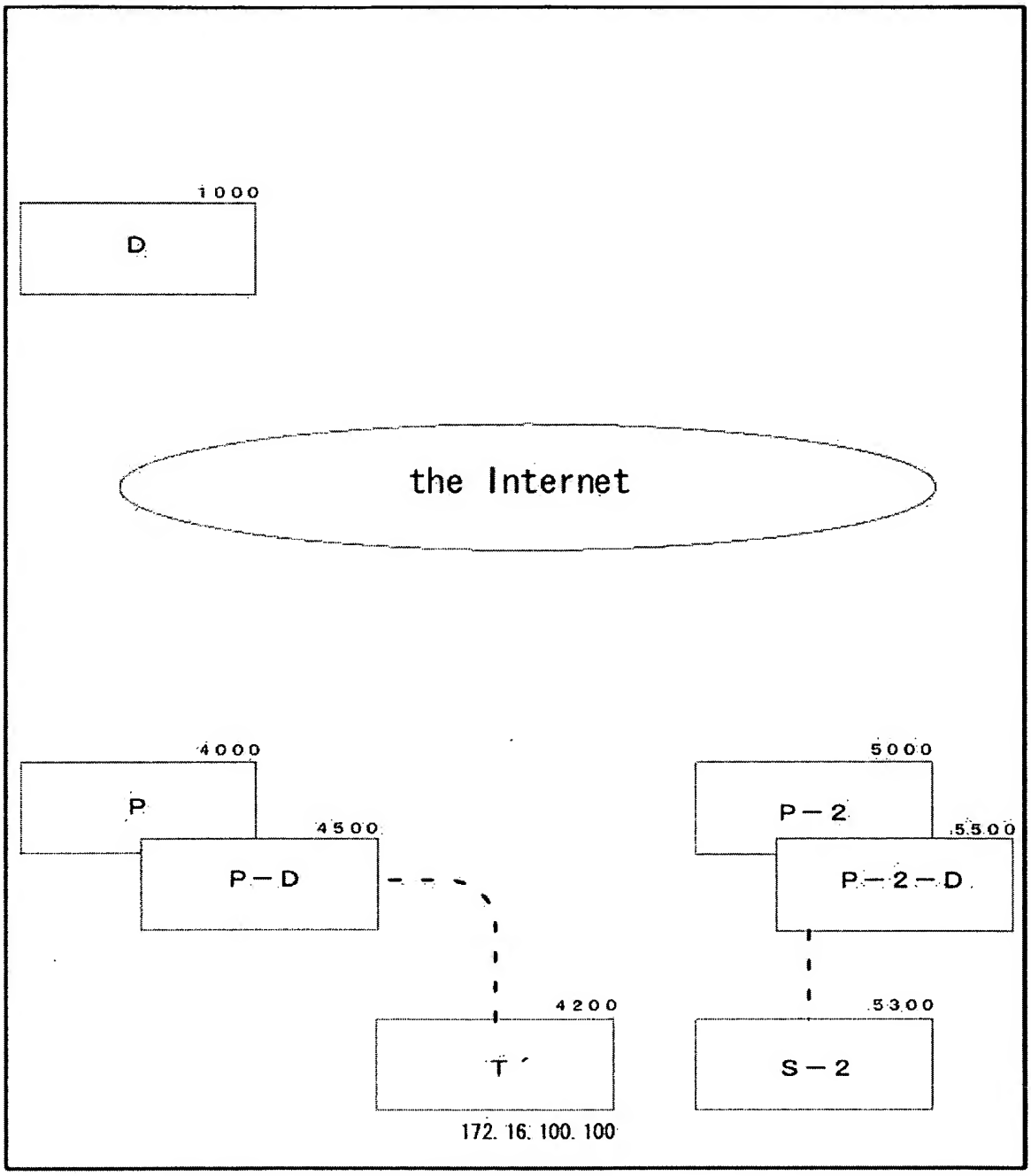

1000
D
the Internet
4000
P
4500
P－D
5000
P－2
5500
P－2－D
4200
T´
5300
S－2
172. 16. 100. 100

図１１

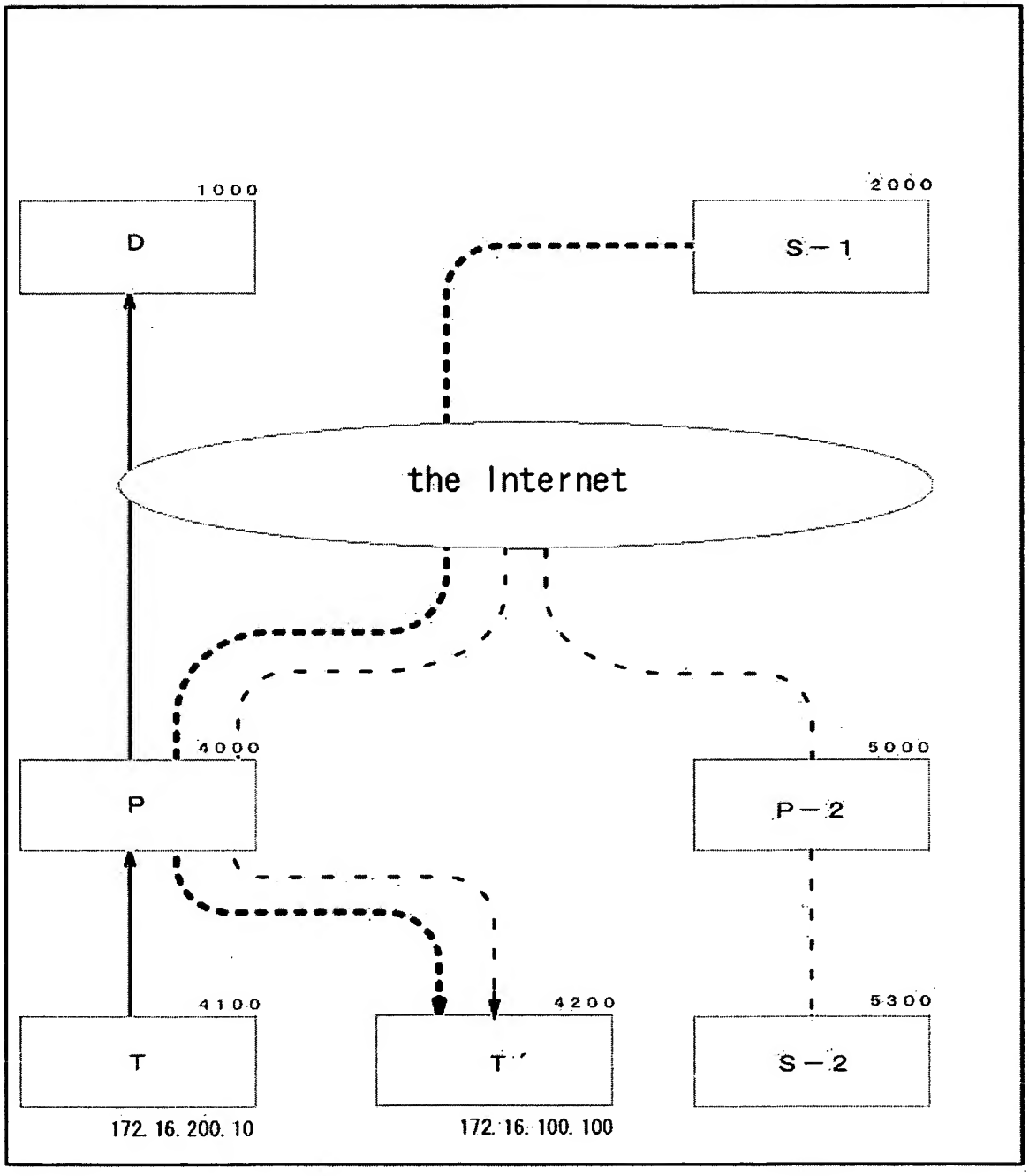

1000
D
2000
S－1
the Internet
4000
P
5000
P－2
4100
T
4200
T'
5300
S－2
172. 16. 200. 10
172. 16. 100. 100

図１２

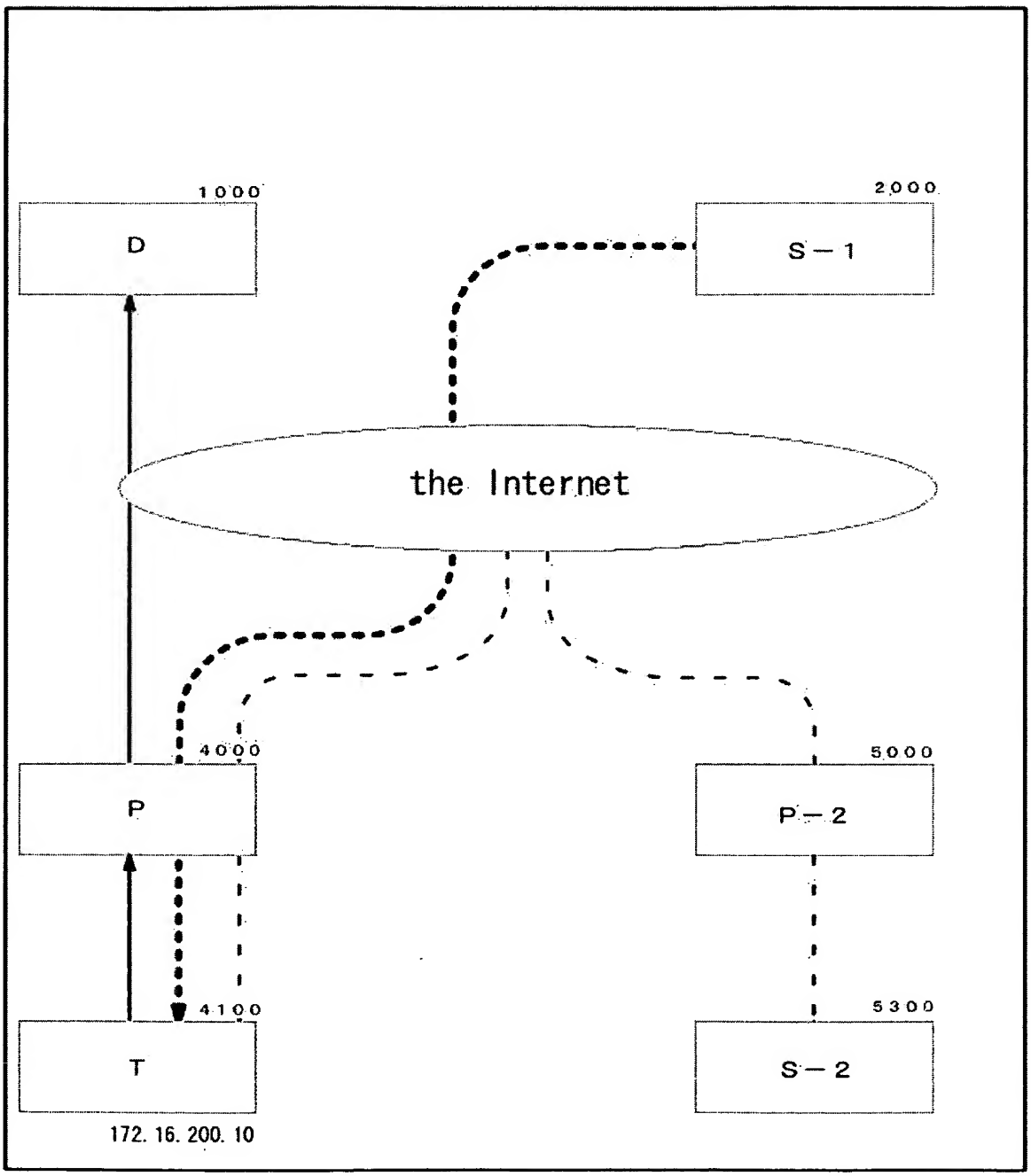

1000
D
2000
S－1
the Internet
4000
P
5000
P－2
4100
T
5300
S－2
172. 16. 200. 10

図１３

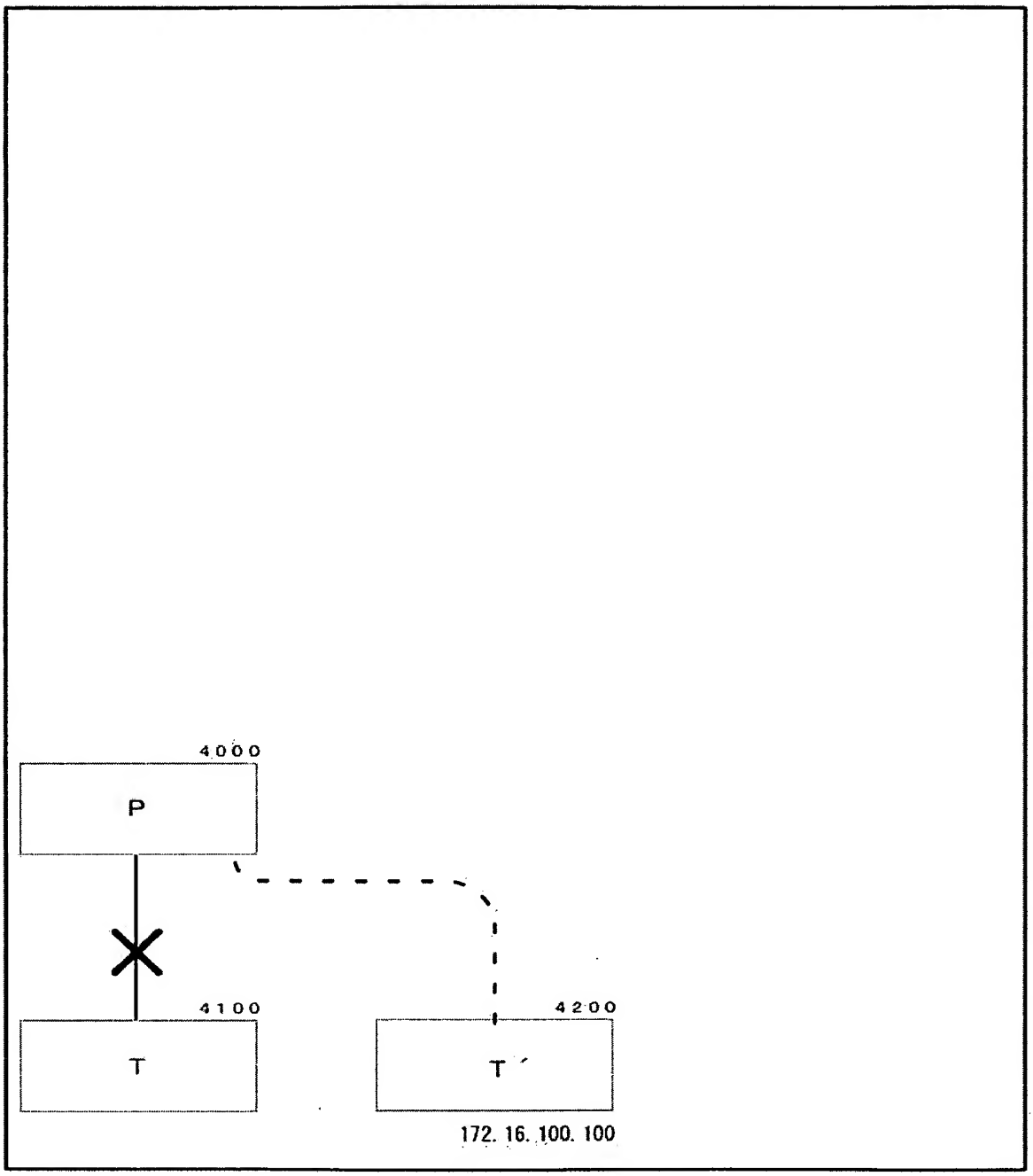


図１４

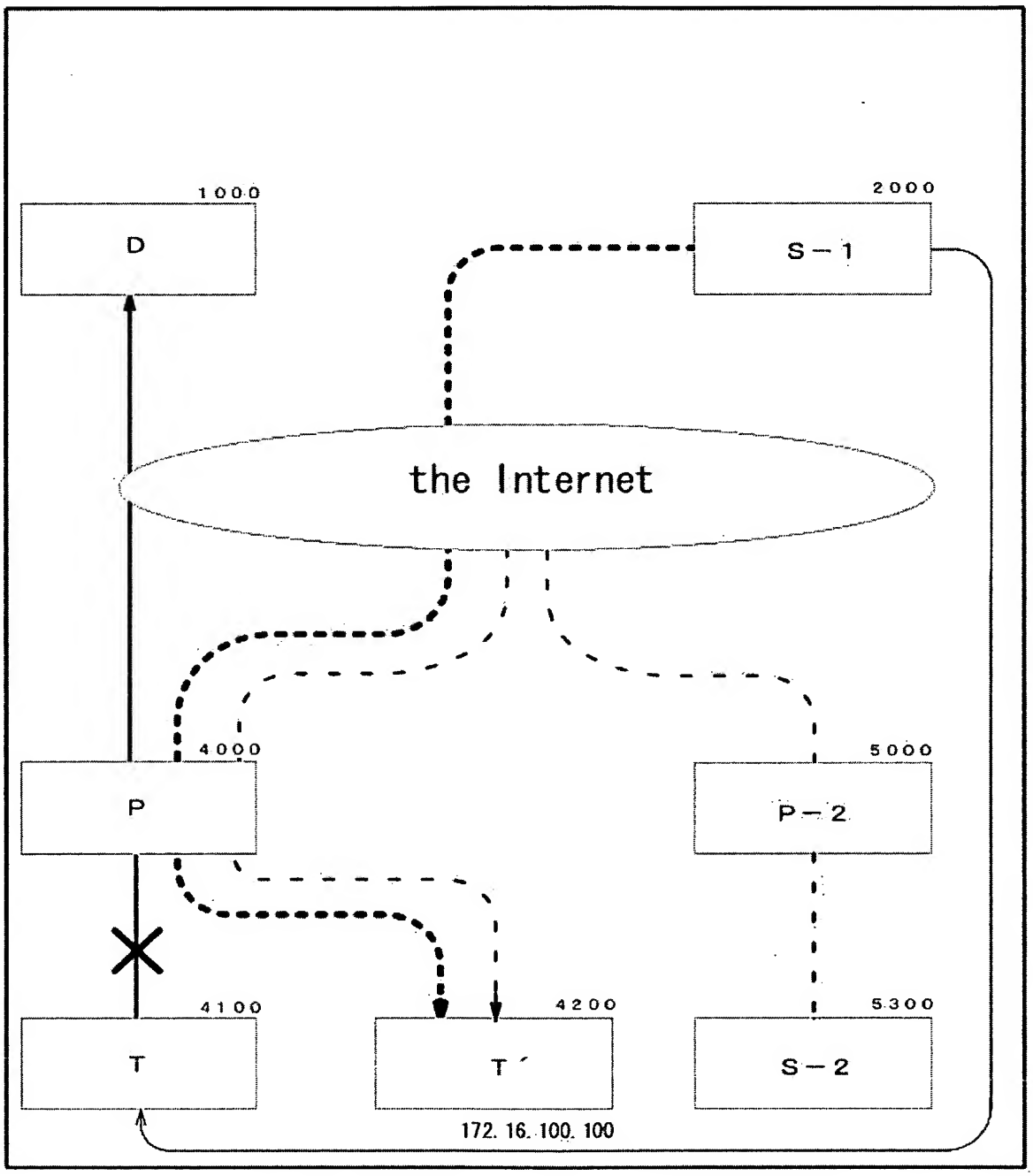

1000
D
2000
S－1
the Internet
4000
P
5000
P－2
4100
T
4200
T´
5300
S－2
172. 16. 100. 100

図１５

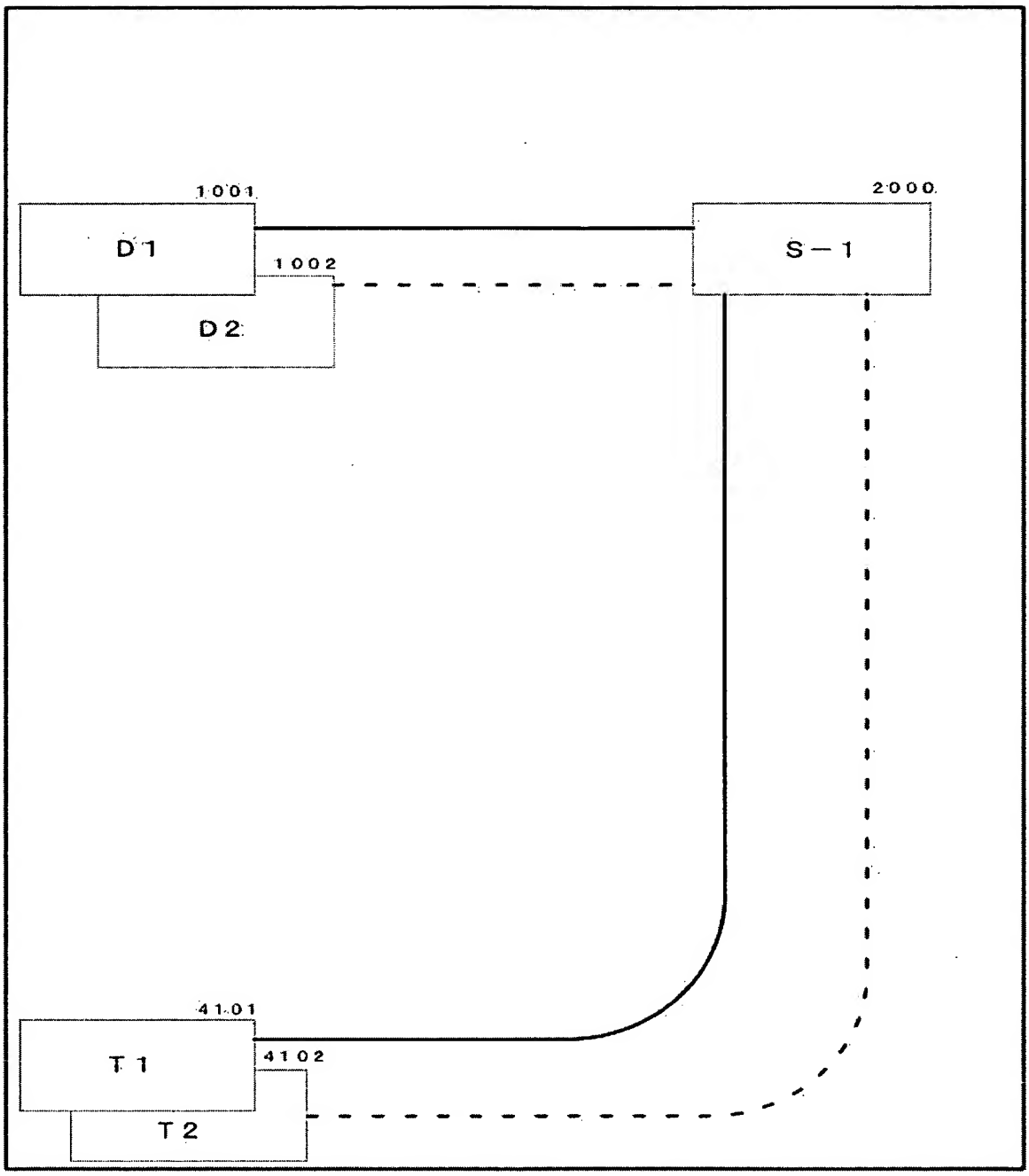


図１６

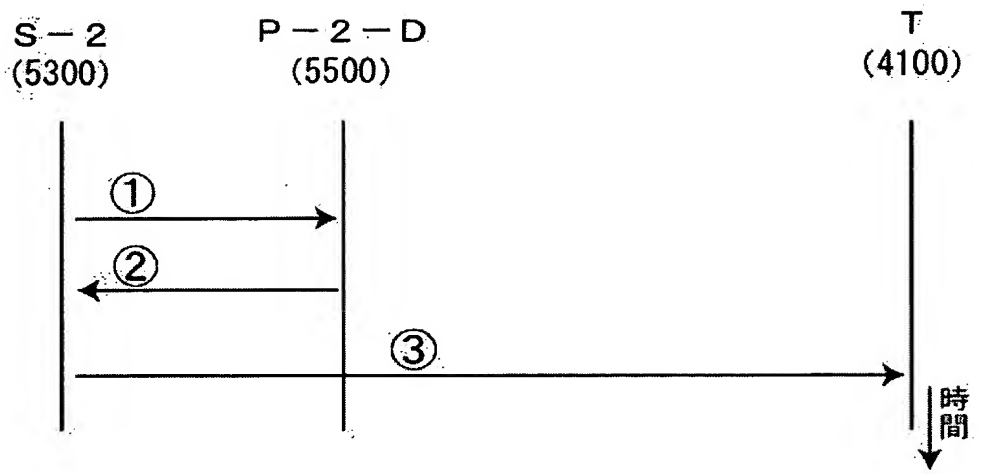

S－2
(5300)
P－2－D
(5500)
T
(4100)
①
②
③
時間

図１７

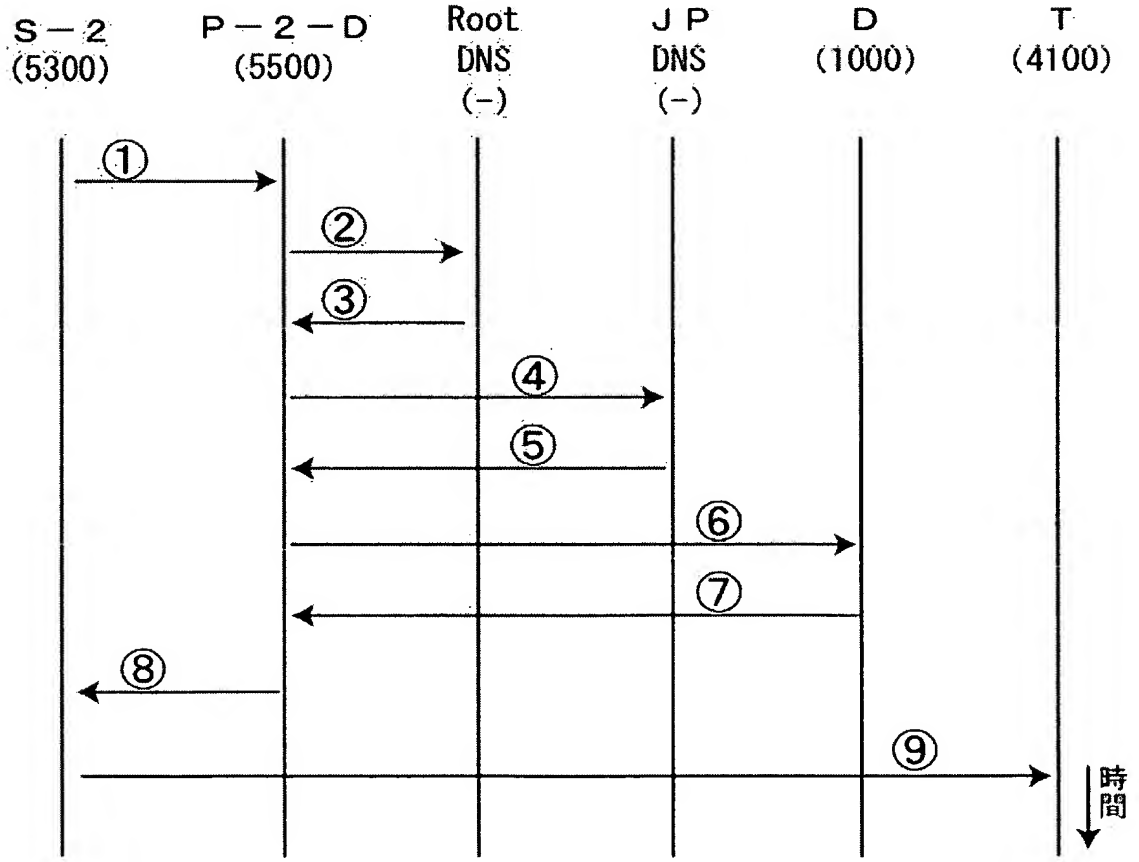

S－2
(5300)
P－2－D
(5500)
Root
DNS
(－)
JP
DNS
(－)
D
(1000)
T
(4100)
①
②
③
④
⑤
⑥
⑦
⑧
⑨
時間

図１８

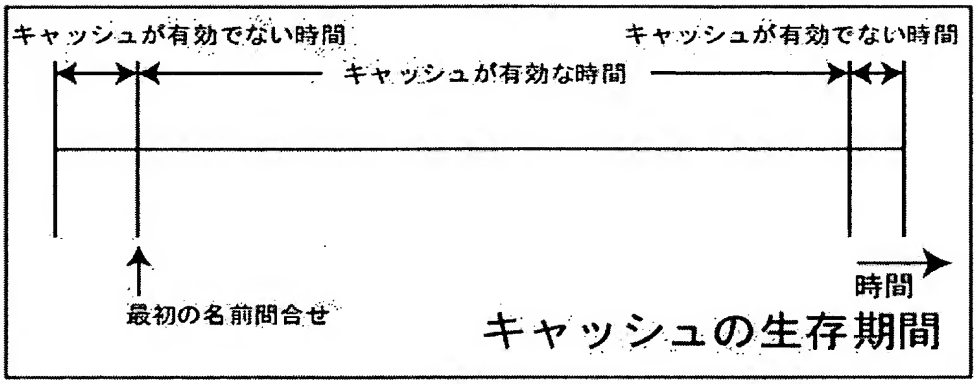


図１９

```
date >> $LOG
echo -n "result od DIG :" >> $LOG
dig @209.69.32.137 bsdguru.dyndns.org | grep bsdguru.dyndns.org | —>
 grep "IN A" | cut -f4 >> $LOG
ping -c 2 bsdguru.dyndns.org >> $LOG
sleep 1
```

図２０

```
1
Thu Sep 12 23:59:36 JST 2002
result od DIG :210.159.30.63 a
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=246 time=70.996 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=246 time=83.131 ms
                              b
--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 70.996/77.064/83.131/6.067 ms


2
Thu Sep 12 23:59:39 JST 2002
result od DIG :218.218.1.196 c
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=246 time=84.041 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=246 time=98.320 ms
                              d
--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 84.041/91.180/98.320/7.139 ms


3
Thu Sep 12 23:59:41 JST 2002
result od DIG :218.218.1.196
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=246 time=91.660 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=246 time=87.170 ms

--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 87.170/89.415/91.660/2.245 ms
```

図２１

```
4
Thu Sep 12 23:59:43 JST 2002
result od DIG :218.218.1.196
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=246 time=87.492 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=246 time=70.174 ms

--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 70.174/78.833/87.492/8.659 ms
```

```
15
Fri Sep 13 00:00:37 JST 2002
result od DIG :218.218.1.196
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=246 time=98.655 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=246 time=81.907 ms

--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 81.907/90.281/98.655/8.374 ms


16
Fri Sep 13 00:00:39 JST 2002
result od DIG :218.218.1.196  e
PING bsdguru.dyndns.org (218.218.1.196): 56 data bytes
64 bytes from 218.218.1.196: icmp_seq=0 ttl=52 time=111.375 ms
64 bytes from 218.218.1.196: icmp_seq=1 ttl=52 time=117.394 ms
                             f
--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 111.375/114.385/117.394/3.010 ms
```

図２２

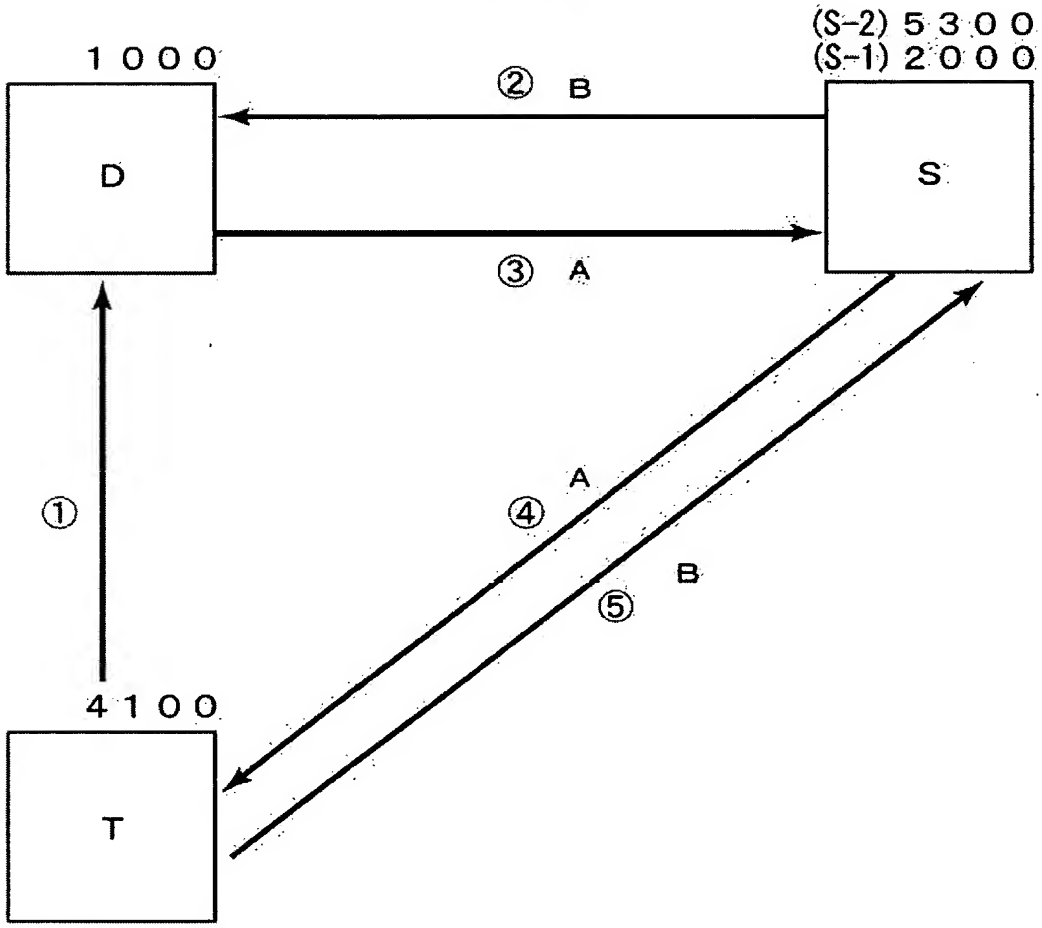


図２３

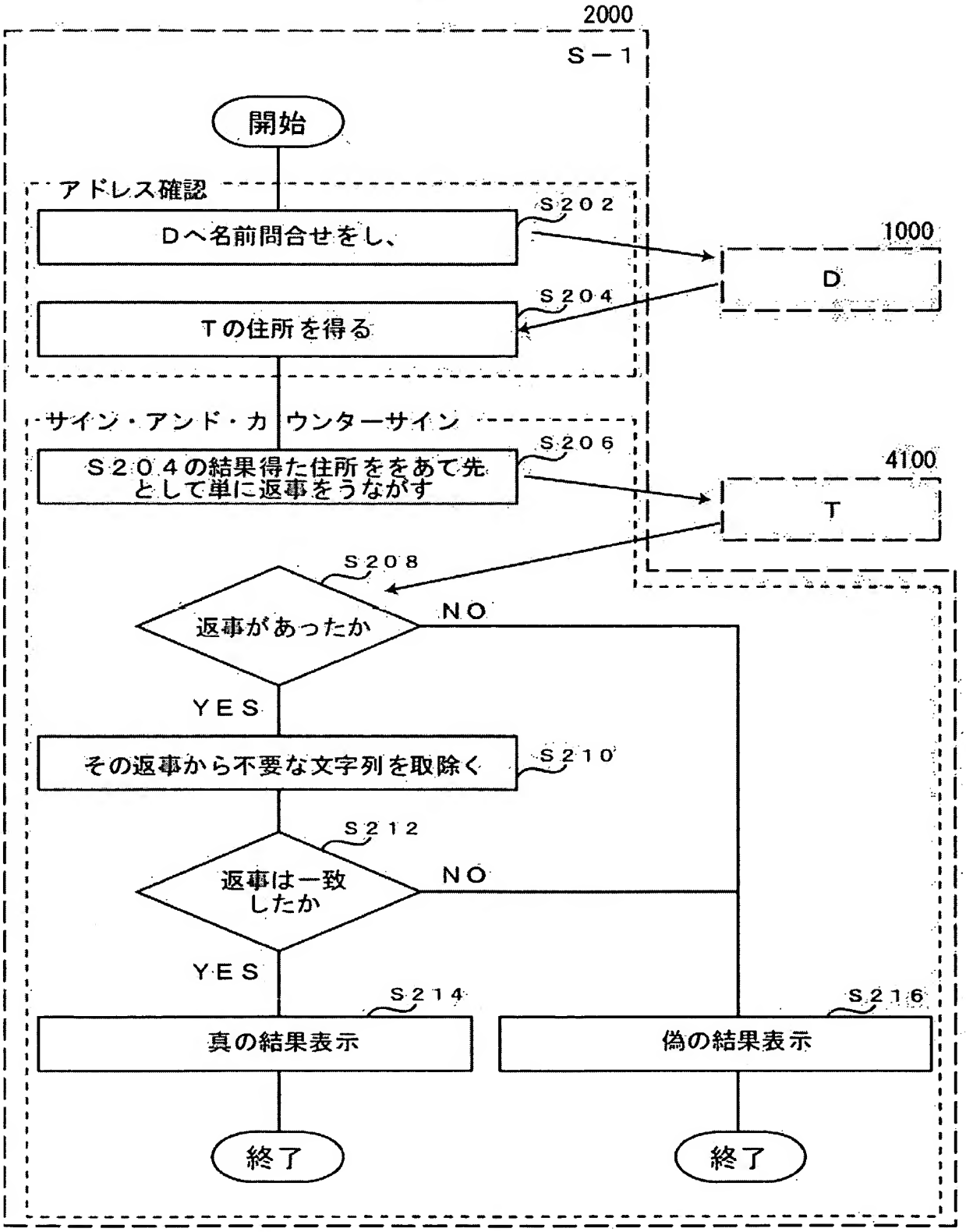

2000
S－1
開始
アドレス確認
S202
Dへ名前問合せをし、
1000
D
S204
Tの住所を得る
サイン・アンド・カウンターサイン
S206
S２０４の結果得た住所ををあて先として単に返事をうながす
4100
T
S208
返事があったか
NO
YES
その返事から不要な文字列を取除く
S210
S212
返事は一致したか
NO
YES
S214
真の結果表示
S216
偽の結果表示
終了
終了

図２４

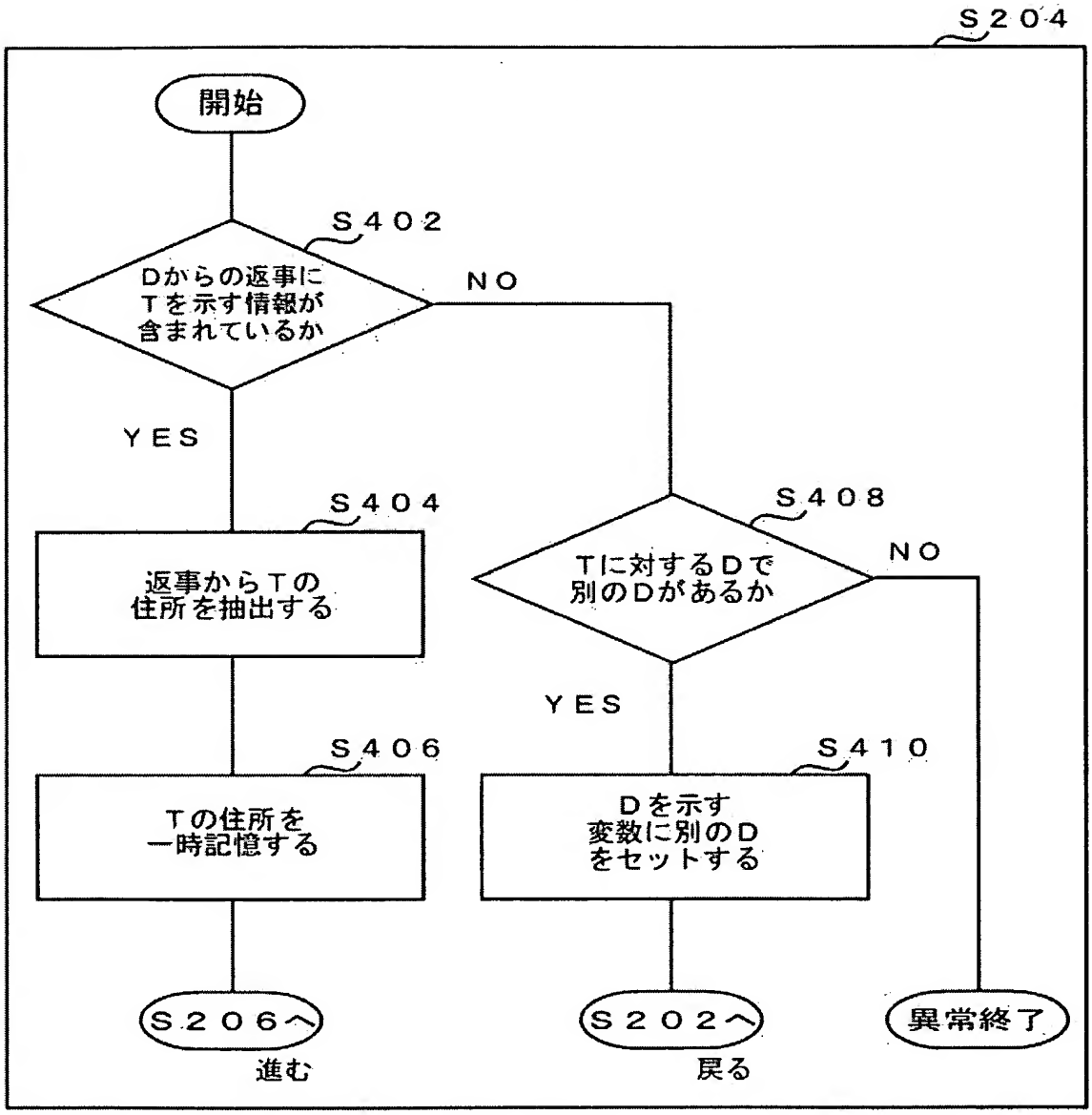

S２０４
開始
S４０２
Dからの返事に
Tを示す情報が
含まれているか
NO
YES
S４０４
返事からTの
住所を抽出する
S４０８
Tに対するDで
別のDがあるか
NO
YES
S４０６
Tの住所を
一時記憶する
S４１０
Dを示す
変数に別のD
をセットする
S２０６へ
進む
S２０２へ
戻る
異常終了

図２５

```
% dig @ns1.dyndns.org bsdguru.dyndns.org

; <<>> DiG 8.3 <<>> @ns1.dyndns.org bsdguru.dyndns.org
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6
;; flags: qr aa rd: QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 5
;; QUERY SECTION:
;;      bsdguru.dyndns.org, type = A, class = IN

;; ANSWER SECTION:
bsdguru.dyndns.org.     1M IN A         218.46.105.100

;; AUTHORITY SECTION:
dyndns.org.             1D IN NS        ns4.dyndns.org.
dyndns.org.             1D IN NS        ns5.dyndns.org.
dyndns.org.             1D IN NS        ns1.dyndns.org.
dyndns.org.             1D IN NS        ns2.dyndns.org.
dyndns.org.             1D IN NS        ns3.dyndns.org.

;; ADDITIONAL SECTION:
ns1.dyndns.org.         1D IN A         66.37.215.43
ns2.dyndns.org.         1D IN A         209.69.32.137
ns3.dyndns.org.         1D IN A         64.71.191.26
ns4.dyndns.org.         1D IN A         212.100.224.171
ns5.dyndns.org.         1D IN A         66.37.215.44

;; Total query time: 231 msec
;; FROM: open.names4commerce.net to SERVER: ns1.dyndns.org  66.37.215.43
;; WHEN: Fri Sep 13 23:24:31 2002
;; MSG SIZE  sent: 36  rcvd: 222
```

図２６

```
% dig @hhh.dyndns.org bsdguru.dyndns.org

; <<>> DiG 8.3 <<>> @hhh.dyndns.org bsdguru.dyndns.org
; (1 server found)
;; res options: init recurs defnam dnsrch                    stderr
;; res_nsend to server hhh.dyndns.org  66.183.188.16: Operation timed out
% echo $status
9
```

図２７

```
% dig @ns1.dyndns.org bsd2guru.dyndns.org

; <<>> DiG 8.3 <<>> @ns1.dyndns.org bsd2guru.dyndns.org
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 6
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUERY SECTION:
;;      bsd2guru.dyndns.org, type = A, class = IN

;; AUTHORITY SECTION:
dyndns.org.             10M IN SOA      ns1.dyndns.org. hostmaster.dyndns.org. (
                                        2057409667      ; serial
                                        10M             ; refresh
                                        5M              ; retry
                                        1W              ; expiry
                                        10M )           ; minimum


;; Total query time: 215 msec
;; FROM: open.names4commerce.net to SERVER: ns1.dyndns.org  66.37.215.43
;; WHEN: Thu Sep 26 22:56:13 2002
;; MSG SIZE  sent: 37  rcvd: 88

% echo $status
0
```

図２８

```
% snmpget 218.46.105.100 public system.sysName.0
system.sysName.0 = bsdguru.dyndns.org
% echo $status
0
```

図２９

```
% snmpget 218.46.105.101 public system.sysName.0
Timeout: No Response from 218.46.105.101.        ～ stderr
% echo $status
1
```

図３０

```
% snmpget 218.46.105.100 wrongcommunity system.sysName.0        ～ stderr
Error in packet
Reason: (noSuchName) There is no such variable name in this MIB.
Failed object: system.sysName.0

% echo $status
2
```

図３１

```
% snmpget 218.46.105.100 public system.sysLocation.0
system.sysLocation.0 = TEST
% echo $status
0
```

図３２

```
options {
directory "/etc/namedb";
// forward only;
forwarders {
127.0.0.1;
};
version="Hyper-Rturner-BOX";
// query-source address * port 53;
// dump-file "s/named_dump.db";
};
```

図３３

```
% dig @218.46.105.100 txt chaos version.bind

; <<>> DiG 8.3 <<>> @218.46.105.100 txt chaos version.bind
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;;      version.bind, type = TXT, class = CHAOS

;; ANSWER SECTION:
VERSION.BIND.           0S CHAOS TXT    "Hyper-Returner-BOX"

;; Total query time: 76 msec
;; FROM: open.names4commerce.net to SERVER: 218.46.105.100
;; WHEN: Thu Sep 26 22:37:43 2002
;; MSG SIZE  sent: 30  rcvd: 73

% echo $status
0
```

図３４

```
% dig @218.46.105.101 txt chaos version.bind

; <<>> DiG 8.3 <<>> @218.46.105.101 txt chaos version.bind
; (1 server found)
;; res options: init recurs defnam dnsrch
;; res_nsend to server 218.46.105.101: Operation timed out
% echo $status
9
```

stderr

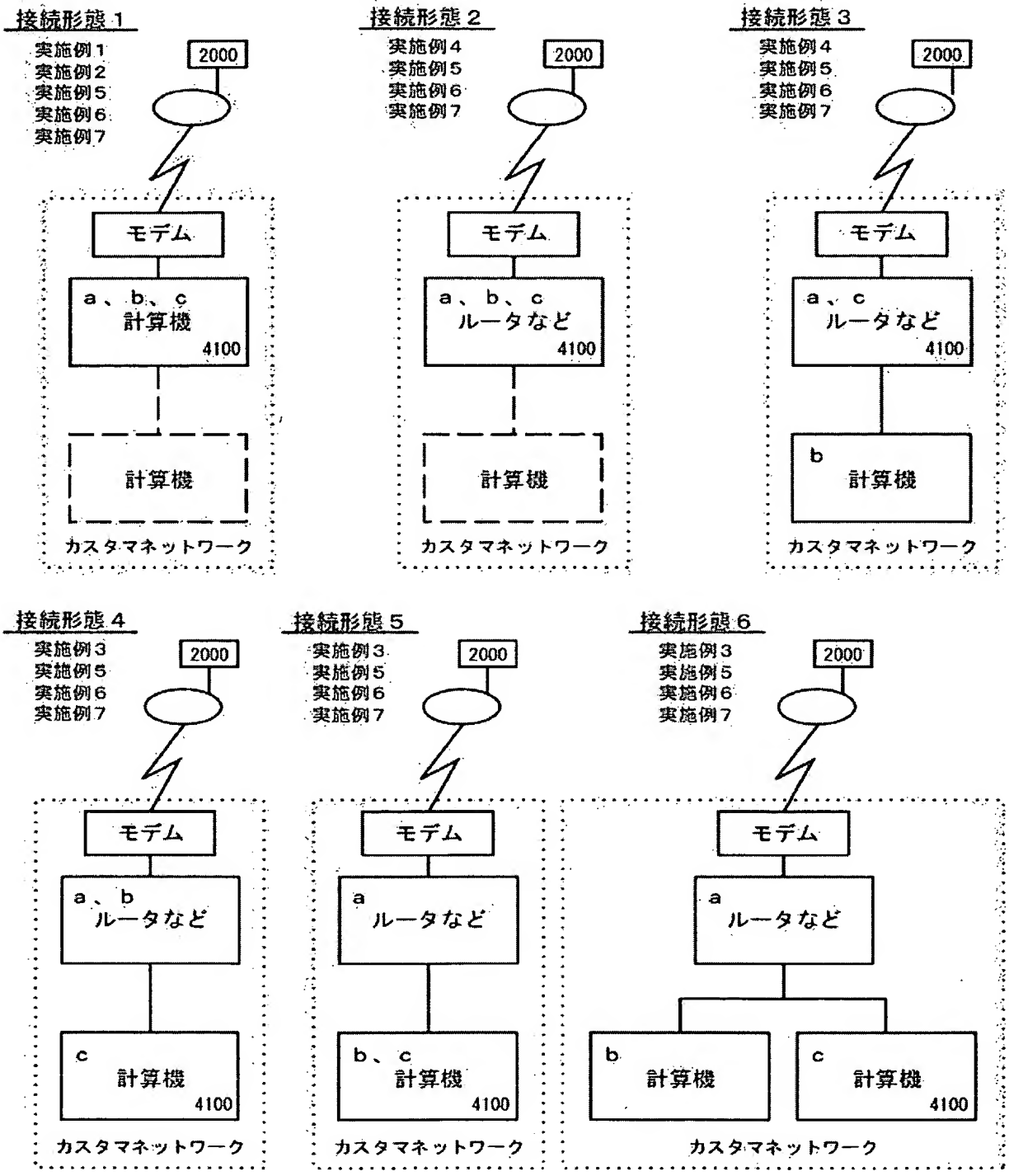
図３５

```
% dig @ns.korai.or.jp txt chaos version.bind

; <<>> DiG 8.3 <<>> @ns.korai.or.jp txt chaos version.bind
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;;      version.bind, type = TXT, class = CHAOS

;; ANSWER SECTION:
VERSION.BIND.           0S CHAOS TXT    "4.9.7-REL"

;; Total query time: 2 msec
;; FROM: open.names4commerce.net to SERVER: ns.korai.or.jp  202.217.175.5
;; WHEN: Thu Sep 26 22:40:57 2002
;; MSG SIZE  sent: 30  rcvd: 64

% echo $status
0
```

図３６

```
Trying 202.217.175.5...
Connected to po.korai.or.jp.
Escape character is '^]'.
220 ns.korai.or.jp ESMTP Sendmail 8.8.8/3.6W-99062802; Tue, 5 Nov 2002 02:14:35
+0900 (JST)
```

図３７



a＝ダイヤルアップする（動的な住所の割当てを受ける）ホスト
b＝D（1000）への更新をするホスト
c＝T（4100）の機能を有するホスト

図３８

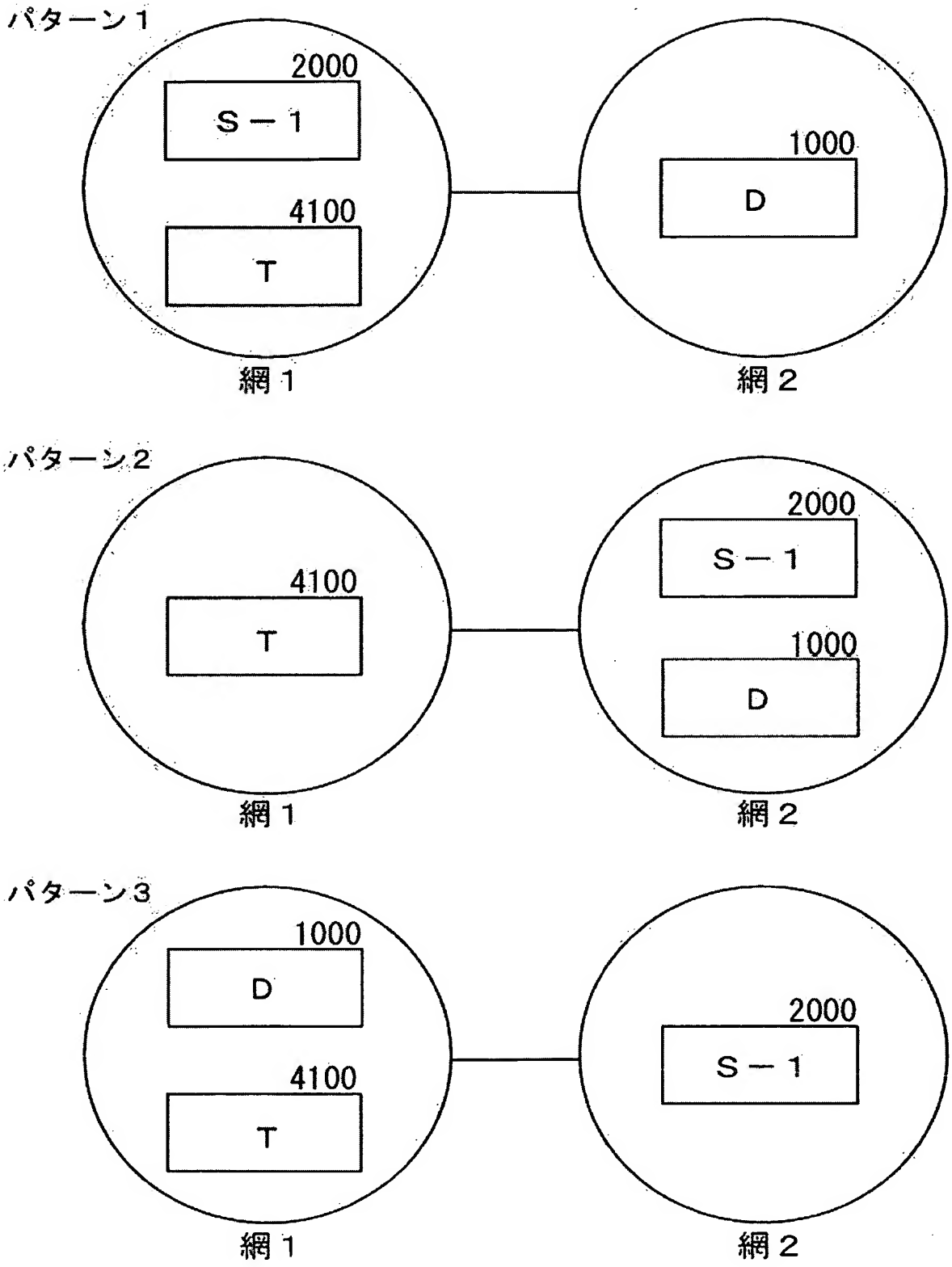

パターン１
2000
S－1
4100
T
1000
D
網１
網２
パターン２
4100
T
2000
S－1
1000
D
網１
網２
パターン３
1000
D
4100
T
2000
S－1
網１
網２

図３９

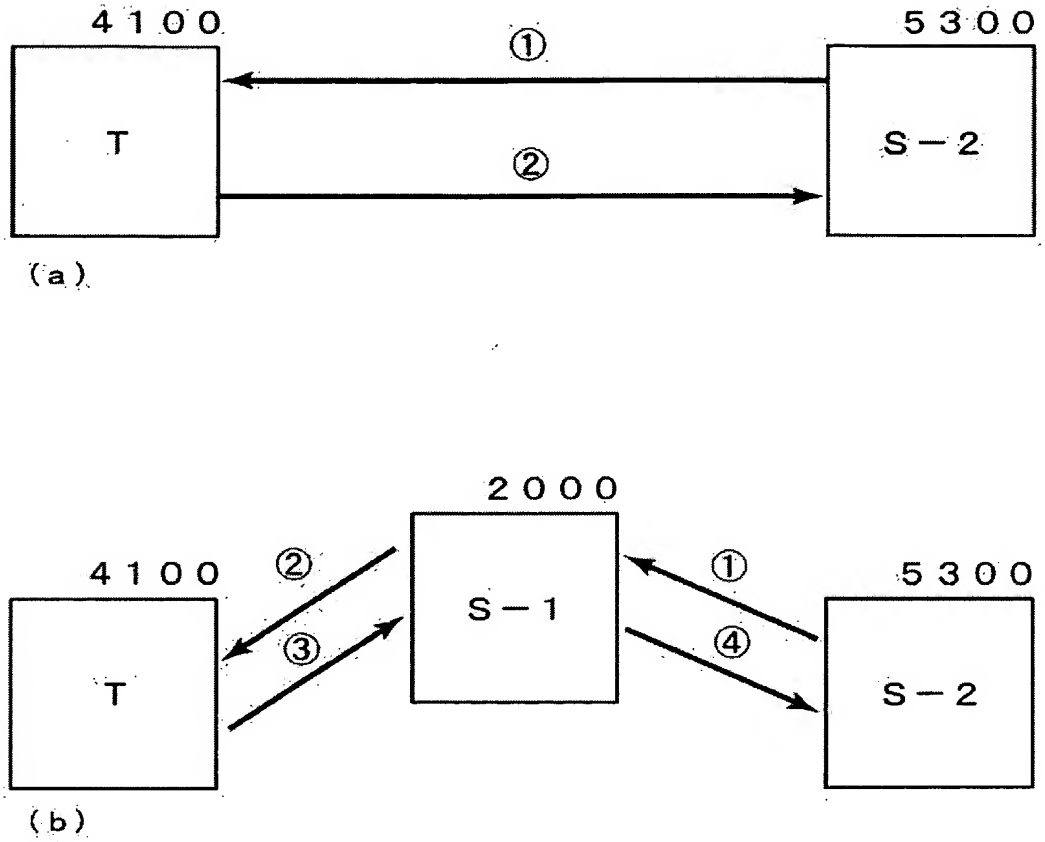
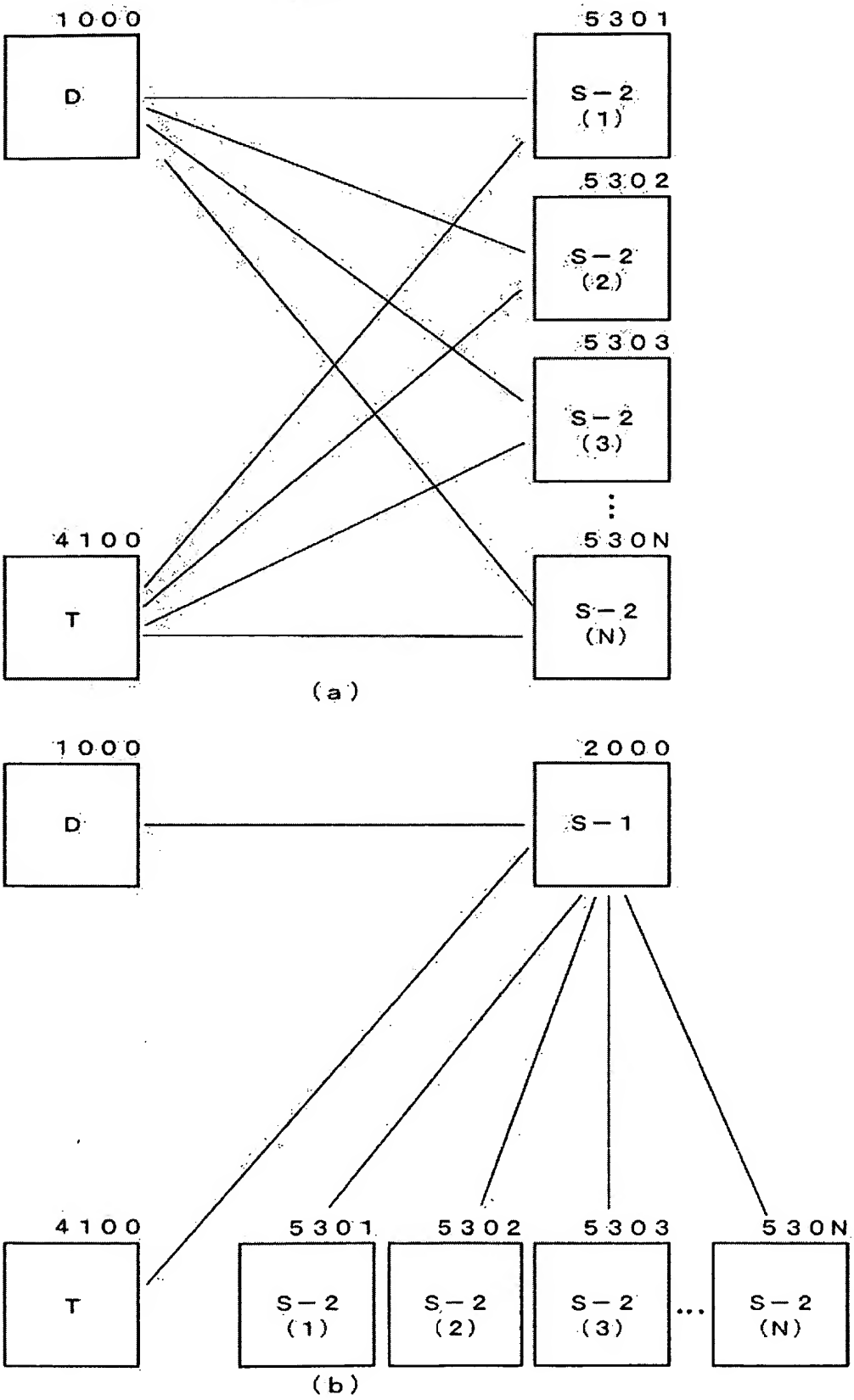


図４０

```
/usr/sbin/nsupdate -k $KEYDIR:$KEYNAME << EOF || $ERRFLG=ERROR
update delete $TARGETHOST A

EOF
```

図４１


1000
D
4100
T
5301
S－2
(1)
5302
S－2
(2)
5303
S－2
(3)
530N
S－2
(N)
(a)
1000
D
2000
S－1
4100
T
5301
S－2
(1)
5302
S－2
(2)
5303
S－2
(3)
530N
S－2
(N)
(b)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/16538

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 2002-135301 A (Nippon Telegraph And Telephone Corp.), 10 May, 2002 (10.05.02), Par. Nos. [0019] to [0031]; Figs. 1, 2 (Family: none)	6-9,12, 15-17,19,22, 23,25,26,42, 43,46-48,51 1-5,10,11, 13,14,18,20, 21,24,27-41, 44,45,49,50
X A	Toshikatsu TAGO, 'Ima kara demo Maniau UNIX & Linux Nyumon Dai 5 Kai Network no Settei (Sono 2)', DB Magazine, Kabushiki Kaisha Shoeisha, Vol.11, No.11, 01 January, 2002 (01.01.02), pages 168 to 174, column of 'nslookup' (page 170)	6,7,42, 44-46,48-51 43,47

[x] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 April, 2004 (06.04.04)	20 April, 2004 (20.04.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/16538

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-318737 A (Kabushiki Kaisha Index), 31 October, 2002 (31.10.02), Par. Nos. [0037] to [0052]; all drawings (Family: none)	1-51
A	JP 11-122283 A (Toshiba Corp.), 30 April, 1999 (30.04.99), Par. Nos. [0029] to [0053]; Figs. 1 to 9 & US 6324577 B1	1-51

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／１６５３８

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Ｉｎｔ．　Ｃｌ⁷　Ｈ０４Ｌ１２／５６

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Ｉｎｔ．　Ｃｌ⁷　Ｈ０４Ｌ１２／５６

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　１９２６－１９９６年
日本国公開実用新案公報　　１９７１－２００４年
日本国登録実用新案公報　　１９９４－２００４年
日本国実用新案登録公報　　１９９６－２００４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	ＪＰ　２００２－１３５３０１　Ａ（日本電信電話株式会社） 2002.05.10 第0019段落から第0031段落，第１，２図 （ファミリーなし）	6-9, 12, 15-17, 19, 22, 23, 25, 26, 42, 43, 46-48, 51
A		1-5, 10, 11, 13, 14, 18, 20, 21, 24, 27-41, 44, 45, 49, 50

[x] C欄の続きにも文献が列挙されている。　　[ ] パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０６．０４．２００４	20.4.2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	玉木　宏治	５Ｘ　３０４７
	電話番号　０３－３５８１－１１０１　内線　３５９６	

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ０３／１６５３８

C（続き）． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	田悟 敏克，「今からでも間に合う ＵＮＩＸ＆Ｌｉｎｕｘ入門 第５回 ネットワークの設定（その２）」，DB Magazine,	6, 7, 42, 44-46, 48-51
A	株式会社翔泳社，第11巻，第11号，2002.01.01，pp.168-174 「nslookup」の項(p.170)	43, 47
A	ＪＰ ２００２－３１８７３７ Ａ（株式会社インデックス） 2002.10.31 第0037段落から第0052段落，全図 （ファミリーなし）	1-51
A	ＪＰ １１－１２２２８３ Ａ（株式会社東芝） 1999.04.30 第0029段落から第0053段落，第１－９図 &US ６３２４５７７ Ｂ１	1-51